PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-193865

(43)Date of publication of application : 28.07.1995

---

(51)Int.Cl. H04Q 7/38
H04M 1/00

---

(21)Application number : 06-170095 (71)Applicant : CASIO COMPUT CO LTD

(22)Date of filing : 28.06.1994 (72)Inventor : HASEGAWA TSUTOMU
SUGIO NAOAKI
MORIYA KOJI
ORIMOTO TAKASHI
KANEKO KATSUYOSHI
WATANABE KAZUYOSHI
HIROYA TAKAYUKI

---

(30)Priority
Priority number : 05252192
05289448
Priority date : 13.09.1993
18.11.1993
Priority country : JP
JP

---

---

(54) PORTABLE TERMINAL EQUIPMENT AND ITS SECURITY METHOD

(57)Abstract:

PURPOSE: To obtain the portable terminal equipment and its security method in which internal data are protected even when the terminal equipment is missing and an impropriety that the terminal equipment is used by a third party and charging is imposed is avoided.

CONSTITUTION: When a PHP 2 is missing, the possessor enters a command by using a key operation section 1b of the telephone set 1 to send remote control data to the PHP 2. The PHP 2 receives the remote control data and an internal protect processing means executes the protect processing excluding disadvantages to the possessor of the PHP 2 based on the received remote control data. As the protect processing, for example, when a third party uses the PHP 2 to make a phone call, the call is connected to a telephone number of a contact place of the possessor of the PHP 2 stored in advance but cannot be connected to any other place or all required data to make a phone call such as ID data of the possessor of the PHP 2 are deleted to make the phone calling not available, or the specific data relating to the possessor of the PHP 2 undesired to be observed by a third party are deleted.

---

---

LEGAL STATUS [Date of request for examination] 26.06.2001

[Date of sending the examiner's decision of rejection] 10.08.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3693259

[Date of registration] 01.07.2005

[Number of appeal against examiner's decision of rejection] 2004-018553

[Date of requesting appeal against examiner's decision of rejection] 09.09.2004

[Date of extinction of right]

the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

CLAIMS

---

[Claim(s)]
[Claim 1] The security approach of the personal digital assistant equipment characterized by performing predetermined protection processing which eliminates that analyze the contents of the remote control data which received remote control data through the communication line, and were received, and the owner of personal digital assistant equipment becomes disadvantageous based on this analysis result from the exterior.
[Claim 2] Personal digital assistant equipment characterized by establishing a protection processing means to perform predetermined protection processing which eliminates that the owner of personal digital assistant equipment becomes disadvantageous, based on the remote control data inputted through the communication line from the exterior.
[Claim 3] Said protection processing means is personal digital assistant equipment according to claim 2 characterized by starting said predetermined protection processing after coincidence of the personal identification number inputted through the communication line from the exterior is checked.
[Claim 4] the protection processing it is made lead to the contact beforehand remembered that A. personal digital assistant equipment is used for said protection processing means, the protection processing which forbids use of B. personal digital assistant equipment, the protection processing which forbids the display of the in-house data of C. personal digital assistant equipment, and ** -- the personal digital assistant equipment according to claim 2 or 3 characterized by to perform at least one or more.
[Claim 5] Personal digital assistant equipment according to claim 4 characterized by establishing further the specific data specification means which can be specified beforehand by using as specific data the in-house data relevant to an owner of personal digital assistant equipment who will be troubled by said personal digital assistant equipment if others see.
[Claim 6] Personal digital assistant equipment characterized by having the means of communications in which data communication is possible, an actuation data recognition means to analyze the transmitted data and to recognize that it is remote control data to this terminal, and a security means to perform predetermined security

processing to this terminal with said remote control data.
[Claim 7] the remote control data which received said security means -- a. -- very much a normal starting sequence A system To the protection processing b. personal digital assistant equipment which is not started The contents of the storage means built [ address / of the outline of continuation or the alarm generating processing d. personal digital assistant equipment generated intermittently ] in the data transmitting processing e. personal digital assistant equipment about which an owner is told in the protection processing c. beep sound which does not output the contents of the storage means built in outside Personal digital assistant equipment according to claim 6 characterized by the thing of all of the protection processings which eliminate the contents of the storage means built in the transmitting processing f. personal digital assistant equipment transmitted to the terminal which has other communication facility, or one or more security processings for which it performs at least any they are.
[Claim 8] It is personal digital assistant equipment according to claim 7 characterized by the thing of all of the protection processings of said a-f, or one or more security processings for which it performs at least any they are when it is the number of setting times have a password input means to enter a password, and a password analysis means to analyze the entered password, and predetermined [ means / said / security ] in the incorrect input of a password.
[Claim 9] The means of communications in which data communication is possible, and a password input means to enter a password, When there are a password analysis means to analyze the entered password, and an incorrect input of a password, the number of predetermined times, a. the contents of the storage means built in the data transmitting processing b. personal digital assistant equipment which tells an owner about the address of the outline of personal digital assistant equipment Personal digital assistant equipment characterized by all of the transmitting processings transmitted to the terminal which has other communication facility, or one or more predetermined things for which it performs at least any they are.
[Claim 10] Personal digital assistant equipment according to claim 8 or 9 characterized by having an incorrect input information means to tell an owner about that there was an incorrect input of a password.
[Claim 11] The security approach of the personal digital assistant equipment characterized by performing security processing which restricts the function of the personal digital assistant equipment concerned if it distinguishes whether it is the no to which this message also receives and a specific signal is in the received signal and this specific signal is detected when the message has also been sent with the call.
[Claim 12] The personal digital assistant equipment characterized by to establish a specific signal-detection means detect a specific signal among said received signals, and a functional limit means will restrict the function of the personal digital assistant

equipment concerned if said specific signal is detected by this specific signal-detection means in the personal digital assistant equipment with a message reception function which this message can also receive when a message has also been sent with a call.

[Claim 13] Said functional limit means is personal digital assistant equipment according to claim 12 carry out the thing of all of the protection processings of the display of the halt e. specification message of the starting d. receiving code output function of the halt c. information function of the reception function of the halt b. usual signal of the input function by a. key input, or the security processing or more of one for which it performs at least any they are as the description.

[Claim 14] Personal digital assistant equipment according to claim 12 characterized by having a specific information storage means to memorize specific information, and a specific information display means to display the specific information memorized by this specific information storage means if said specific signal is detected by said specific signal detection means.

[Claim 15] Said specific information storage means is personal digital assistant equipment according to claim 14 characterized by having memorized the contents which tell contacts, such as a name of the owner of the service firm using personal digital assistant equipment, and personal digital assistant equipment, the address, and the telephone number.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to personal digital assistant equipment and its security approach, and relates to the security approach that disadvantageous profit of an owner can be prevented, to loss and the theft of the personal digital assistant equipment which made it possible to perform internal control of the body of personal digital assistant equipment from the exterior by the remote control in detail, and personal digital assistant equipment.

[0002]

[Description of the Prior Art] Digital radio personal digital assistant equipment is known, for example, PHP (Personal Handy Phone), PDA (Personal Digital Assistant), etc. are one of typical things of current personal digital assistant equipment. It

connects with a public line network through the base station installed in the outdoors, and PHP etc. can extend the communication link range by carrying out to the outdoors.

[0003]

[Problem(s) to be Solved by the Invention] By the way, even if others acquired the lost personal digital assistant equipment when personal digital assistant equipment itself was lost outdoors for example, if it was in conventional personal digital assistant equipment, it was possible to have used it as it is, and in spite of could consider the case turned to the contractor of personal digital assistant equipment about the claim of phonecall charges and having not used it, there was a fault that it was necessary to pay a tariff. Even if it prevented from using the personal digital assistant equipment lost through the entrepreneur (for example, so-called NTT, so-called DDI, etc.) side who form the network of public correspondence, moreover, only by it becoming impossible to use the message function of a telephone Personal digital assistant equipment did not necessarily return to an owner's hand, and there was a fault that it might be known by others about the important data inside personal digital assistant equipment (for example, individual telephone number data).

[0004] Then, this invention aims at offering the security approach that disadvantageous profit of the personal digital assistant equipment and the owner who can prevent the fault at the time of losing can be prevented.

[0005]

[Means for Solving the Problem] The security approach of the personal digital assistant equipment by invention according to claim 1 is characterized by performing predetermined protection processing which eliminates that analyze the contents of the remote control data which received remote control data through the communication line, and were received, and the owner of personal digital assistant equipment becomes disadvantageous based on this analysis result from the exterior for the above-mentioned purpose achievement. Personal digital assistant equipment according to claim 2 is characterized by establishing a protection processing means to perform predetermined protection processing which eliminates that the owner of personal digital assistant equipment becomes disadvantageous, based on the remote control data inputted through the communication line from the exterior.

[0006] It considers as a desirable mode, for example, after coincidence of the personal identification number into which said protection processing means was inputted through the communication line like from the exterior according to claim 3 is checked, said predetermined protection processing may be started. moreover -- for example, the protection processing it is made lead to the contact according to claim 4 beforehand remembered that A. personal digital assistant equipment is used for said protection processing means like, the protection processing which forbids use of B. personal digital assistant equipment, the protection processing which forbids the

display of the in-house data of C. personal digital assistant equipment, and ** -- it may be made to perform at least one or more. For example, the specific data specification means which can be specified beforehand may be further established by using as specific data the in-house data relevant to an owner of personal digital assistant equipment according to claim 5 who will be troubled by said personal digital assistant equipment like if others see.

[0007] Personal digital assistant equipment according to claim 6 is characterized by having the means of communications in which data communication is possible, an actuation data recognition means to analyze the transmitted data and to recognize that it is remote control data to this terminal, and a security means to perform predetermined security processing to this terminal with said remote control data. For example like claim 7 publication, moreover, said security means the received remote control data -- a. -- very much a normal starting sequence A system To the protection processing b. personal digital assistant equipment which is not started The contents of the storage means built [ address / of the outline of continuation or the alarm generating processing d. personal digital assistant equipment generated intermittently ] in the data transmitting processing e. personal digital assistant equipment about which an owner is told in the protection processing c. beep sound which does not output the contents of the storage means built in outside Even if there is little all of the protection processings which eliminate the contents of the storage means built in the transmitting processing f. personal digital assistant equipment transmitted to the terminal which has other communication facility, or one or more security processing, it may be made to perform any they are.

[0008] For example, it has a password input means according to claim 8 to enter a password like, and a password analysis means to analyze the entered password, and when there is an incorrect input of a password the predetermined number of setting times, said security means may be made to perform any they are, even if there is little all of the protection processings of said a-f or one or more security processing. The means of communications in which the data communication of personal digital assistant equipment according to claim 9 is possible, and a password input means to enter a password, When there are a password analysis means to analyze the entered password, and an incorrect input of a password, the number of predetermined times, a. It is characterized by all of the transmitting processings which transmit the contents of the storage means built in the data transmitting processing b. personal digital assistant equipment which tells an owner about the address of the outline of personal digital assistant equipment to the terminal which has other communication facility, or one or more predetermined things for which it performs at least any they are. For example, you may make it have an incorrect input information means to tell an owner about a thing [ that there was an incorrect input of a password ] according to claim 10 like.

[0009] If the security approach of personal digital assistant equipment according to claim 11 distinguishes whether it is the no to which this message also receives and a specific signal is in the received signal and this specific signal is detected when the message has also been sent with the call, it will be characterized by performing security processing which restricts the function of the personal digital assistant equipment concerned. Personal digital assistant equipment according to claim 12 is characterized by to establish a specific signal-detection means detect a specific signal among said received signals in the personal digital assistant equipment with a message reception function which this message can also receive, and a functional limit means will restrict the function of the personal digital assistant equipment concerned if said specific signal is detected by this specific signal-detection means, when a message has also been sent with a call.

[0010] For example, even if few in all of the protection processings of the display of the halt e. specification message of the starting d. receiving code output function of a halt [ of the reception function of the halt b. usual signal of an input function according / said functional limit means / to a. key input like ] c. information function according to claim 13, or the security processing or more of one, it may be made to perform about any they are. For example, you may make it have a specific information storage means according to claim 14 to memorize specific information like, and a specific information display means to display the specific information memorized by this specific information storage means if said specific signal is detected by said specific signal detection means. For example, you may make it have memorized the contents which tell contacts, such as a name of the owner of the service firm according to claim 15 said whose specific information storage means uses personal digital assistant equipment like, and personal digital assistant equipment, the address, and the telephone number.

[0011]

[Function] In this invention, when personal digital assistant equipment is lost, that owner or a communication link entrepreneur inputs remote control data through a communication line, and protection processing which eliminates that the owner of personal digital assistant equipment becomes disadvantageous with a **** stylish protection processing means at this remote control data is performed. Processing which it is made to lead to the contact beforehand remembered to use personal digital assistant equipment, for example as protection processing, forbids use of personal digital assistant equipment, or forbids the display of the in-house data of personal digital assistant equipment is performed. Therefore, even if it loses personal digital assistant equipment, the fault of protection of the data inside personal digital assistant equipment being possible, and it being used for others and charged can be prevented by the command from an owner or a communication link entrepreneur.

[0012] Moreover, in invention given [ other ] in a claim, if the incorrect input of a

password is detected on the occasion of use even if it does not collect to an owner the owner data which, and connect the whereabouts to an owner or are memorized and an owner does not notice loss of a terminal to the actuation and use in personal digital assistant equipment based on the remote control data transmitted from the exterior, security processing will be performed. [ data ] [ protect ] Therefore, even when personal digital assistant equipment is lost or a theft is suited, the event which becomes disadvantageous to an owner can be removed, and useful data can be collected. Furthermore, in invention given [ other ] in a claim, if it distinguishes whether it is the no which has a specific signal in the received signal and a specific signal is detected, security processing which restricts the function of the personal digital assistant equipment will be performed. Therefore, when the situation which is not expected between an owner and personal digital assistant equipment occurs (for example, loss, a theft), by transmitting a specific signal using a dial-up line from the exterior, communication facility can be restricted and the danger of being abused for the 3rd person can be abolished.

[0013]

[Example] Hereafter, the example of this invention is explained with reference to a drawing.

1st example drawing 1 of this invention and drawing 2 are drawings showing the 1st example of the personal digital assistant equipment concerning this invention, and are the example applied to PHP (Personal Handy Phone).

A. Network configuration drawing 1 of a PHP system is the network configuration Fig. of a PHP system. As for the communication line by which the telephone by which 1 was connected to the public line network (PSTN, ISDN), and 2 were connected to PHP as a portable telephone, and 3 was connected to the public line network (PSTN, ISDN), and 4, in drawing 1 , a relay base office and 5 are radio circuits. Moreover, 4a is the antenna of a relay base office, and 21 is the antenna (refer to drawing 2 ) of PHP2. The call of PHP2 and a mutual message are possible for telephone 1 through the radio circuit 5 from the relay base station 4 which was installed by an office, domestic, or the public, was connected to the public line network, for example, in the city and various suburban messages were possible, and also was further connected to the public line network. Sequential arrangement is carried out for every comparatively small-scale area, and the relay base office 4 mainly forms the radio circuit 5 to PHP2, and performs control which makes a message possible between PHP2 and other telephones.

[0014] Control unit switch 1b which inputs into telephone 1 the command which carries out the remote control of the input and PHP2 of the telephone number etc. to headset (hand set) 1a is arranged. Moreover, control unit switch 1b can input now a personal identification number including ten digits or a notation. in this case, only when the below-mentioned coincidence acknowledge signal which shows that the

predetermined value beforehand remembered to be a receiving personal identification number from PHP2 was in agreement is transmitted to telephone 1 and telephone 1 receives this coincidence acknowledge signal, a remote control entry of data is received (for example, remote control data input receptionist mode is permitted) -- it is like.

[0015] B. The PHP block block diagram 2 is a block diagram showing the detailed configuration of PHP2. In drawing 2 , 11 is a control section which controls the whole equipment according to a predetermined protocol, and consists of CPUs etc. A control section 11 controls various kinds of actuation of the digital cordless telephone equipment as PHP which includes voice data transmitting processing using RAM13 which memorizes data, the result of an operation, etc. temporarily according to the micro program stored in ROM12. Moreover, when the remote control data with which the control section (protection processing means) 11 was transmitted from telephone 1 in the case of this example are received, control for performing predetermined protection processing which eliminates that the owner of PHP2 becomes disadvantageous based on this received remote control data is performed.

[0016] The contents of protection processing are as follows.

Mode A : When the telephone number of the owner who memorized in memory 17 beforehand is displayed on the below-mentioned display 15 and PHP2 is lost, When others are going to telephone temporarily using the lost PHP2, All the data that are needed when telephoning, such as ID data of the owner of protection processing-mode B:PHP2 which is altogether connected with the place of the telephone number of the contact of the owner of PHP2 memorized beforehand, are eliminated. Protection processing-mode C others prevent from telephoning: Selection in protection processing-mode A which eliminates the specific data relevant to an owner of PHP2 who will be troubled if others see - Mode C has composition performed by operating control unit switch 1b by the side of telephone 1. In addition, as long as it eliminates that do not restrict the contents of protection processing to the above-mentioned example, and the owner of PHP2 becomes disadvantageous, you may be other contents of protection. For example, in Mode B, it is made not to receive the signal from the key input section 14 which PHP2 mentions later, or the display of specific data may be forbidden in software in Mode C.

[0017] The display 15 which consists of LCD which displays the key input section 14, the addresser number and time of day when a ten key and various kinds of function keys were formed, duration of a call, phonecall charges, etc. on a control section 11, and the response message currently recorded beforehand are sent out, and the rec/play circuit 16 which consists of the cassette tape or IC memory which records the business from a partner etc., and the memory 17 which memorizes the various data containing voice data are connected. When a control section 11 receives the personal identification number transmitted from telephone 1 and both are in

agreement here as compared with the predetermined value (personal identification number) beforehand memorized by memory 17 in this personal identification number that received, While performing control which transmits the coincidence acknowledge signal which shows that it was in agreement to telephone 1, after transmitting this coincidence acknowledge signal at least, various kinds of protection processings (Mode A - Mode C) mentioned above based on the remote control data transmitted from telephone 1 are started. Therefore, a control section 11 has a function as a coincidence command means.

[0018] Moreover, the key input section 14 has the function as a specific data specification means which can be specified beforehand by using as specific data the data relevant to an owner of PHP2 who will be troubled if others see. As specific data, there are the telephone number of an individual home, a customer's telephone number, a bank account number, etc., for example. When the specific data specification input which specifies the purport these [ whose ] are specific data while being able to operate the key input section 14 and being able to make memory 17 memorize beforehand is possible for these specific data, it was specified as specific data and protection processing in Mode C is chosen as mentioned above, storage of memory 17 is eliminated by the control section 11.

[0019] C. Explain transmission/receiving network of PHP, next transmission/receiving network of PHP2. The radio-frequency head 22 which carries out frequency conversion of the sound signal which carried out digital modulation with the modem 23 to a transceiver radio frequency (RF), and is emitted in the air from an antenna 21 or PHP2 receives the signal of the transceiver radio frequency (RF) frequency band from an antenna 21, The modem 23 which carries out digital modulation of the sound signal in which TDMA processing was carried out by the TDMA signal-processing section 24 or it carries out the digital recovery of the sound signal which carried out RF reception, The TDMA signal-processing section 24 which performs TDMA (Time Division Multiple Access: time division multiple access) processing which carries out time sharing of the radio frequency, and transmits a transceiver signal in the shape of a burst in a specific time zone, The speech codec 25 which performs compression/elongation processing for a digital sound signal, The PCM codec 26 which encodes and outputs the sound signal inputted by the telephone transmitter 29 to a PCM digital signal or it changes a digital signal into an analog signal and outputs to an earphone 28 through amplifier 27, It is constituted by the earphone 28 which consists of a loudspeaker etc., the telephone transmitter 29 which consists of a microphone etc., and the ringer section 30 which sounds a ringer.

[0020] The above-mentioned radio-frequency head 22 carries out frequency-conversion processing, and consists of antenna switches 35 which distribute a receive section 31, the transmitting section 32, the PLL synthesizer 33, a band pass filter 34, and transmission/reception. A receive section 31 does frequency

conversion of the RF signal which was received by the antenna 21 and inputted through the band pass filter 34 and the antenna switch 35 by two steps of mixers, makes it the signal of a 150-250MHz frequency band from 1.9GHz, and does frequency conversion to the intermediate frequency (IF) signal near 10 moreMHz. The transmitting section 32 carries out frequency conversion of the modulated wave of pi / 4 shift QPSK inputted from the modem 23 to 1.9GHz by the mixer, and radiates it from an antenna 21 through the antenna switch 35 and a band pass filter 34.

[0021] The PLL synthesizer 33 carries out local oscillation for frequency conversion in a receive section 31 and the transmitting section 32. The above-mentioned modem 23 carries out strange recovery processing of pi / 4 shift QPSK, and in a receiving side, it restores to the IF signal from a receive section 31, and separates into IQ signal, and it transmits it to the TDMA signal-processing section 24 as a data stream. Moreover, in a transmitting side, IQ signal is created from the data transmitted from the TDMA signal-processing section 24, pi / 4 shift QPSK is modulated, and it outputs to the transmitting section 32.

[0022] The above-mentioned TDMA signal-processing section 24 carries out frame synchronization and format processing of a slot. That is, in a receiving side, the data of the slot addressed to self are picked out from a modem 23 or the data sent to predetermined timing, a scramble etc. is canceled, configuration data are taken out from a format of this slot, control data is transmitted to a control section 11, and delivery and voice data are transmitted to the speech codec 25. In a transmitting side, it is predetermined timing, namely, it inserts in the self-quota slot of a frame and sends out to a modem 23, adding control data to the voice data transmitted from the speech codec 25, creating transmit data, and applying a scramble etc.

[0023] Moreover, the TDMA signal-processing section 24 sends and receives the signal of the same frequency so that it may not lap in time between base stations 4, it processes it so that it may communicate mutually, and transmission and reception of a signal are performed using the time amount location (time slot) of the pair assigned in the TDMA frame of the fixed length who becomes a primitive period. Each station sends out a signal to the time slot to which it was assigned in the frame, and it performs that time amount position control (burst synchronousr control) so that this signal may not collide with other signals.

[0024] The speech codec 25 carries out compression/elongation processing of digital data. That is, in a receiving side, it elongates by decrypting the ADPCM sound signal (4 bitx8kHz=32k bps) sent from the TDMA signal-processing section 24 to a PCM sound signal (8 bitx8kHz=64k bps), and outputs to the PCM codec 26. In a transmitting side, it compresses by encoding the PCM sound signal sent from the PCM codec 26 to an ADPCM sound signal, and outputs to the TDMA signal-processing section 24. The PCM codec 26 carries out an analog / digital transform processing. In a receiving side, D/A conversion of the PCM sound signal sent from the speech codec 25 is carried

out, an analog sound signal is outputted to amplifier 27, and a loudspeaker 28 is driven. In a transmitting side, A/D conversion of the analog sound signal inputted from the microphone 29 is carried out, and a PCM sound signal is outputted to the speech codec 25. Moreover, volume / ringer / tone signal is controlled.

[0025] Next, an operation is explained.

D. The whole communication link actuation telephone 1 is installed by an office, domestic, or the public, and in the city and various suburban messages are performed from connecting with a public line network through a communication line 3. Moreover, the call of PHP2 and a mutual message are performed through the radio circuit 5 from the relay base station 4. In this case, a large number are arranged one by one for every comparatively small-scale area, the relay base office 4 mainly forms the radio circuit 5 to PHP2, and control which makes a message possible between PHP2 and other telephones is performed.

[0026] E. The whole PHP the access method and transmission system in PHP2 of this example of operation have adopted the TDMA/TDD communication mode, time sharing also of two or more terminals by time sharing, communicate going up / the data getting down was carried out, and they has put them on the same frequency. That is, the voice from the distant office (for example, telephone 1 and other terminal telephone equipments) transmitted through the relay base station 4 is changed into baseband signaling by the radio-frequency head 22 through an antenna 21, and is received, a digital recovery is carried out by the modem 23, and the received sound signal is outputted to the TDMA signal-processing section 24. The TDMA signal-processing section 24 changes into the original transmission speed the signal sent in the shape of a burst, and takes out a sound signal while it controls the timing of reception so that the digital sound signal received based on the control signal (a subcarrier synchronization, a bit synchronization, frame alignment signal) added to the sending signal does not collide with the signal at the time of transmission. The speech codec 25 develops, the digital sound signal taken out by the TDMA signal-processing section 24 is changed into an analog sound signal by the PCM codec 26, and sound emission is carried out from an earphone 28 through amplifier 27.

[0027] On the other hand, the sound signal inputted from the telephone transmitter 29 is encoded by the PCM digital signal by the PCM codec 26, the data compression of the encoded digital signal is carried out by the speech codec 25, and it is outputted to the TDMA signal-processing section 24. The TDMA signal-processing section 24 outputs the burst signal which performs the burst transmission control which transmits a signal in the shape of a burst, and is transmitted by predetermined transmit timing to a modem 23. Digital modulation of the sending signal inputted into the modem 23 is carried out here, it is outputted to a radio-frequency head 22, and frequency conversion is carried out to a radio frequency by the radio-frequency head 22, and it is emitted in the air through an antenna 21. Moreover, a change and

condition in the mode are controlled based on the keypad information from the key input section 14, and while outputting the burst control signal for making a transmitting output into a burst wave to the burst control signal input terminal of the transmitting section 32 of a radio-frequency head 22, when the status signal based on a control result is sent out to a display 15 or the arrival from the TDMA signal-processing section 24 is received, it controls sounding a ringer 30 etc. by the control section 11. After the electric wave emitted in the air is caught by antenna 4a of the relay base station 4 through the radio circuit 5 and is processed in the relay base station 4, it is transmitted to telephone 1 through a communication line 3, and it is received by telephone 1.

[0028] F. Explain protection processing actuation, next the protection processing actuation which is the description part of this example. First, when an owner loses PHP2, the owner (namely, true owner) operates key stroke section 1b of telephone 1, and telephones PHP2. If PHP2 gets a telephone call, the mutual communication line network which can transmit and receive data will be formed between telephone 1 and PHP2. At this time, there is lost PHP2 to those (henceforth an acquisition person) who acquire and own it in many cases. Subsequently, the owner of PHP2 operates key stroke section 1b, selects personal identification number input mode, and inputs a predetermined personal identification number (it is "#11223344#" at a ten-digit number). It may replace with a personal identification number, for example, the ID code of the owner of PHP2 may be used.

[0029] If a personal identification number is inputted, when both are in agreement as compared with the predetermined value (for example, the same value as a personal identification number) which memorized the personal identification number which received in memory 17 beforehand, by the PHP2 side, the coincidence acknowledge signal which shows that it was in agreement will be transmitted to telephone 1. By telephone 1, only when a coincidence acknowledge signal is received, a remote control entry-of-data receptionist is attained. Subsequently, the owner of PHP2 operates key stroke section 1b, and inputs a remote control command. In the PHP2 side, any of protection processing or the activation in (Mode A, Mode B, or Mode C) which eliminates that the owner of PHP2 becomes disadvantageous based on the remote control data corresponding to this remote control command is started. In addition, if a control section 11 is not after transmitting the coincidence acknowledge signal mentioned above, it will not start protection processing.

[0030] (-- when "Mode A" chooses as selection, for example, protection processing, of a) "Mode A", the telephone number of the owner who memorized in memory 17 beforehand displays on a display 15, and when others (acquisition person) try to telephone using lost PHP2, the processing which leads to the place of the telephone number of the contact of the owner of PHP2 memorized beforehand altogether is performed. Therefore, the situation which an acquisition person says telephones

freely can be prevented, and it can suppress being turned to the contractor of PHP2 about the claim of phonecall charges to the minimum. consequently, in spite of not using it, the fault of avoiding the situation without payment trap ****** where there is nothing, using a tariff for others, and being charged can be prevented. Moreover, since it is altogether connected with the place of the telephone number of the contact of the owner of PHP2 in this case, supposing the acquisition person of PHP2 has telephoned, the owner of PHP2 can also request that PHP2 should be returned to an acquisition person, and is very convenient. That is, since it is return-easy in a true owner's hand and can be made it, returning to a true owner's hand is also possible in practice.

[0031] (-- when "Mode B" is chosen as selection, next protection processing of b) "Mode B", all the data that are needed when telephoning, such as ID data of the owner of PHP2, are eliminated, and protection processing whose others prevent from telephoning is performed. Therefore, even if it tries in order that an acquisition person may telephone using PHP2, a telephone cannot be made, but the situation of telephoning freely can be prevented, and the fault of it being used for others like the above and charged can be prevented.

[0032] (-- as selection and protection processing of c) "Mode C", when "Mode C" is chosen, protection processing which eliminates the specific data relevant to a true owner of PHP2 who will be troubled if others see is performed. However, the telephone function is permitted only by selection in "Mode C." Therefore, all of the telephone number of the individual home specified beforehand, a customer's telephone number, a bank account number, etc. are eliminated. Consequently, it can carry out by not being known by others about important data. That is, protection of important data can be aimed at. Thus, many problems produced by the remote control from telephone 1 when PHP2 is lost are appropriately clearable.

[0033] Although this example is an example which applied personal digital assistant equipment to PHP, as for this invention, it is needless to say that it is broadly applicable not only to PHP but other personal digital assistant equipments (for example, cordless telephone machine for home use). Moreover, not only the example of the above-mentioned example but other approaches may be used for the method of checking the same possession nature between telephone 1 and PHP2. For example, the personal identification number for protection corresponding to each protection processing may be prepared, the same owner and the contents of protection processing may be transmitted to coincidence, and may be checked, and a personal identification number and the contents of control may be added to the special ID code for carrying out protection processing. Furthermore, it cannot be overemphasized that what kind of thing is sufficient as the class and the number of each part material which constitutes equipment, the control approach, etc. It is good to perform the same protection processing as this invention by the remote control as for a method of

****** by there being nothing from telephone 1 and inputting a predetermined personal identification number etc. as an expansive gestalt of this invention, even from the public telephone which it is usually also in where in case of emergency.

[0034] The 2nd example of this invention, next the 2nd example of this invention are explained.

A. The block diagram 3 of a network system is drawing showing the network system of the personal digital assistant equipment which applied this invention. In drawing 3 , 51 is the public/leased line network, and the public/leased line network here are common telephone public networks. Two or more base stations 54-56 and net control stations 57 the common telephone 52, the personal computer 53 through a modem, and for personal digital assistants are connected to the public / leased line network 51. The personal digital assistant is connected to two or more base stations 54-56 through wireless, respectively. That is, a base station 54 is connected to the pocket mold computer 61 through wireless, a base station 55 is connected to a portable telephone 62 through wireless, and the base station 56 is further connected to the pager 63 through wireless. As a pocket mold computer 61, the small computer of a tele terminal mold or a PAMUTO top mold is used, for example. As a portable telephone 62, what is sold in PHP or two or more of each company, for example (for example, cellular FON) is used. The thing of the type of NP, IP, etc. is used as a pager 63. A net control station 57 manages the whole network, and performs control to each personal digital assistant.

[0035] B. the configuration of a protection circuit -- here, this example explains the example which added the protection equipment which realizes a security function to the portable telephone 62. The configuration of the hard principal part is the same as that of what is shown in drawing 2 of the 1st example mentioned above, in addition protection equipment is added in this example. Protection equipment performs the control for performing predetermined security processing in which the factor which becomes disadvantageous to the owner of a portable telephone 62 based on this remote control data is deleted, when the remote control data transmitted by the owner are received, and the control for performing input / analysis processing of a password, and carries out the control for performing the security processing set up also to the mistaken input. A portable telephone 62 realizes the function of means of communications, an actuation data recognition means, a security means, and a password analysis means.

[0036] Next, an operation is explained.

C. Main routine drawing 4 of security processing and 5 are flow charts which show the main routine which realizes the protection feature (security processing) in protection equipment.

(a) When the owner of the control portable telephone 62 of the protection equipment by the owner loses the portable telephone 62 or suits a theft, the control routine of

the security processing shown in drawing 4 is performed. That is, in step S10, the owner of a portable telephone 62 inputs remote control data that a communication link should be started to the portable telephone 62 owned using the personal computer 53 connected through the modem to the net control station 57. At this time, the contents of the remote control data transmitted with the significance of the information memorized to a situation and the interior when a portable telephone 62 is lost are chosen. The control code is added to remote control data, and the personal identification number which only an owner knows is contained. Therefore, the 3rd person cannot send remote control data to arbitration to an owner's portable telephone 62. Thereby, improper use of a remote control can be prevented.

[0037] On the other hand, even if case or held, when it is not the system whose owner of a portable telephone 62 does not hold the personal computer 53 and which can be accessed through a modem to a net control station 57, transmission of remote control data is requested from the base station 55 of a portable telephone 62 with voice the common telephone 52 (for example, telephone of individual possession). Or remote control data are inputted by the push circuit using telephone 52. Subsequently, the remote control data which the owner of a portable telephone 62 inputted are transmitted to the base station 55 of a portable telephone 62 through the public / leased line network 51 at step S12. Subsequently, it progresses to step S14 and remote control data are transmitted on radio from the base station 55 of a portable telephone 62 (T shows transmission of data). Thus, the remote control data inputted from the personal computer 53 are sent to the base station 55 of a portable telephone 62 through the public / leased line network 51, and a net control station 57, and are transmitted to the target portable telephone 62. In addition, if the portable telephone 62 has the function of two-way communication, a link will be established and it will transmit that reception by the side of a portable telephone 62 was ensured to the personal computer 53 which an owner operates.

[0038] (b) If processing of processing drawing 4 of the remote control data in a personal digital assistant is performed and remote control data are transmitted to a portable telephone 62 on radio from a base station 55, the manipulation routine of the remote control data in the personal digital assistant shown in drawing 5 will be performed. First, the wake rise of the system is carried out at step S20 by reception of remote control data (in drawing 5 , it simplifies with remote data). Thereby, in a portable telephone 62, the system of security processing starts except for a display (for example, protection equipment etc. starts). Subsequently, it distinguishes whether it is remote control data to itself (portable telephone 62) at step S22. This is judged including coincidence of a personal identification number. When the personal identification number is different when it is not its remote control data or, a system is turned off and it returns to the normal mode (return).

[0039] It is its remote control data, and when the personal identification number is in

agreement, it progresses to step S24, and the contents of remote control data are analyzed. In detail, the code is assigned to remote control data, respectively for every processing "communication facility protection", the "contents display protection of storage", "an owner contact display", "alarm sound generating", "prohibition of power-on", the "contents transmission of storage", and "whereabouts area transmission of a terminal", it branches in the code, and concrete processing is started. That is, it distinguishes whether the analysis result of the contents of remote control data is the code of "communication facility protection" at step S26, and it branches to step S28 at the time of YES, and it performs processing of "communication facility protection." Processing of "communication facility protection" is later mentioned by the subroutine. About other processings, it mentions later by the subroutine similarly. It progresses to step S30 at step S26 at the time of NO.

[0040] At step S30, it distinguishes whether the analysis result of the contents of remote control data is the code of "the contents display protection of storage", and it branches to step S32 at the time of YES, and it performs processing of "the contents display protection of storage." It progresses to step S34 at step S30 at the time of NO. At step S34, it distinguishes whether the analysis result of the contents of remote control data is the code of an "owner contact display", and it branches to step S36 at the time of YES, and it performs processing of an "owner contact display." It progresses to step S38 at step S34 at the time of NO.

[0041] At step S38, it distinguishes whether the analysis result of the contents of remote control data is the code of "alarm sound generating", and it branches to step S40 at the time of YES, and it performs processing of "alarm sound generating." It progresses to step S42 at step S38 at the time of NO. At step S42, it distinguishes whether the analysis result of the contents of remote control data is a code "against power-on", and it branches to step S44 at the time of YES, and it performs processing "against power-on." It progresses to step S46 at step S42 at the time of NO. At step S46, it distinguishes whether the analysis result of the contents of remote control data is the code of "the contents transmission of storage", and it branches to step S48 at the time of YES, and it performs processing of "the contents transmission of storage." It progresses to step S50 at step S46 at the time of NO. At step S50, it distinguishes whether the analysis result of the contents of remote control data is the code of "whereabouts area transmission of a terminal", and it branches to step S52 at the time of YES, and it performs processing of "whereabouts area transmission of a terminal." A system is turned off at step S50 at the time of NO, and it returns to the normal mode (return).

[0042] D. Explain the subroutine of each concrete protection processing based on the analysis result of the subroutine of security processing, next the contents of remote control data.

** Subroutine drawing 6 of "communication facility protection" is a flow chart which shows the subroutine of "communication facility protection." If it shifts to this subroutine, the flag against a communication link is turned on at step S100. Since the flag against a communication link stands by this when performing processing with reference to a flag, the communication facility of a portable telephone 62 stops. Therefore, even when the owner of a portable telephone 62 loses the portable telephone 62 or suits a theft, the 3rd person can communicate and fault -- the owner of a portable telephone 62 is burdened with an excessive claim -- can be prevented. If it passes through step S100, it will return to the normal mode.

[0043] ** Subroutine drawing 7 of "the contents display protection of storage" is a flow chart which shows the subroutine of "the contents display protection of storage." If it shifts to this subroutine, the latch who does the disable of the user storage area selection signal at step S110 is turned on. If it passes through step S110, it will return to the normal mode. Thereby, access to a user storage area (an owner's private data and due to occupational cases secret data are memorized) is forbidden. When remote control data are received, it becomes impossible therefore, to obtain only data without semantics which it says altogether is [FFh" or "00h", even if the control signal which chooses the corresponding user storage area always serves as a disable and the 3rd person accesses. Consequently, even if it is the case where an owner's private data and due to occupational cases secret data are memorized, it can prevent it being published by the 3rd person or being abused. Moreover, you may make it eliminate the data in a user storage area at this time. Since there are no data displayed by this even if it accesses a user storage area, it can prevent it being published by the 3rd person or being abused.

[0044] ** Subroutine drawing 8 of an "owner contact display" is a flow chart which shows the subroutine of an "owner contact display." If it shifts to this subroutine, the display of a display is turned on at step S120. Thereby, the display by the display is attained. Subsequently, an owner contact as shown in drawing 9 is expressed to a display as step S122. Drawing 9 is an example of a display at the time of losing a personal digital assistant device, and a name, the address, and the telephone number are displayed. When it loses by mislaying of a portable telephone 62 etc., it enables the person who acquired the portable telephone 62 to the owner to connect by issuing this display. However, since a possibility that the cell of built-in in a portable telephone 62 may be turned off is in the inside which is not attached to the public notice when a display is indicated without ON ****** here, processing which erases a display automatically after fixed time amount progress is performed.

[0045] That is, it distinguishes whether the timer was counted at step S124 and the setup time (for example, 1 hour) passed at step S126. If the setup time has not passed, it returns to step S124, a loop formation is repeated and the setup time passes, it escapes to step S128 and the display of a display is turned off. Thereby, the display of

an owner contact disappears. If it passes through step S128, it will return to the normal mode. Thus, by performing processing which erases a display automatically after fixed time amount progress, a required display can be performed preventing consumption of a cell and the owner contact to the 3rd person can be advertized. If the person who followed, for example, acquired the portable telephone 62 can contact an owner, it will become possible for me to also have you return to an owner. In addition, after it makes it display intermittently for example or an owner transmits remote control data, you may make it display an owner contact during a certain 1 scheduled time only once. Moreover, it uses together with "alarm sound generating" of step S40, and you may make it sound an alarm sound. If it is made such, an owner contact can be more effectively advertized to the 3rd person.

[0046] ** Subroutine drawing 10 of "alarm sound generating" is a flow chart which shows the subroutine of "alarm sound generating." If it shifts to this subroutine, the flag of alarm sound generating is turned on at step S150. Since the flag of alarm sound generating stands by this when performing processing with reference to a flag, an alarm sound (for example, loudspeaker) will occur from a portable telephone 62, and a perimeter will be told. Therefore, when the owner of a portable telephone 62 loses the portable telephone 62 or suits a theft, by transmitting remote control data, the alarm sound of a portable telephone 62 can be sounded remotely, and the abnormal condition about a portable telephone 62 can be reported. ** which can also notice the portable telephone 62 which hears it as a result, for example, an alarm sound, and has the 3rd person in a loss location (for example, on the street) If it passes through step S150, it will return to the normal mode.

[0047] ** Subroutine drawing 11 "against power-on" is a flow chart which shows the subroutine "against power-on." If it shifts to this subroutine, the flag (power-on switch disable flag) which carries out the disable of the power-on switch at step S160 is turned on. If it passes through step S160, it will return to the normal mode. By this, the instruction which forbids the power-on of a portable telephone 62 itself will be executed. That is, since the power-on switch disable flag stands, even if it makes it a manual and turns ON the switch of a portable telephone 62, the microcomputer of a control section checks this flag in a power-on sequence, when remote control data are received, if a flag is ON, will interrupt power-on processing and will change to OFF immediately. Therefore, although the owner who is not even if a portable telephone 62 is used for other persons and it uses connection fees may be charged when a portable telephone 62 suits a theft By interrupting power-on processing like this example, it can change into the condition that it cannot be immediately used even if it is in a theft, and the 3rd person can communicate and fault -- the owner of a portable telephone 62 is burdened with an excessive claim -- can be prevented. For example, although it is the system which contacts a contractor and I have suspend the use when a credit card is lost, the owner of a portable telephone 62 can perform same processing

immediately.

[0048] ** Subroutine drawing 12 of "the contents transmission of storage" is a flow chart which shows the subroutine of "the contents transmission of storage." If it shifts to this subroutine, the portable telephone 62 which received this command at step S200 will establish a link between the terminals (the assignment terminal is described in the control code) which an owner specifies. In this case, a link with the personal computer 53 connected to the public / leased line network 51 by the modem will be established. Subsequently, the contents of storage are transmitted to a personal computer 53 from a portable telephone 62 at step S202. The contents of storage here mean the stored data, when data, such as a case where it does not have backup files, such as an individual scheduler, an individual address book, etc., and data on the business inputted at the destination, to collect are memorized by the portable telephone 62.

[0049] By performing processing of step S202, it becomes possible to upload to the terminal which an owner specifies. Subsequently, a personal computer 53 distinguishes whether it received correctly at step S204 (based on a receipt signal from a personal computer 53). If it has not received correctly, and it returns to step S202, a receiving loop formation is repeated and it receives correctly, by performing processing which clears the contents of storage at step S206, the transmitted data will be cleared and it will return to the normal mode. In addition, to use together with other data protection processings, step S206 does not necessarily need to be data cleared. It checks that the contents of storage of a portable telephone 62 were copied or transmitted, and data have been copied or transmitted without an error to the storage (for example, a floppy disk or a hard disk) of a personal computer 53 from the portable telephone 62 by this, and this actuation is completed. Therefore, when a portable telephone 62 suits a theft, or even when a portable telephone 62 is lost, data, such as data without backup files, such as an individual scheduler, an individual address book, etc., and data on the business inputted at the destination, to collect can be easily copied or transmitted to the storage of their own personal computer 53 from a portable telephone 62, and loss of precious data can be prevented.

[0050] ** Subroutine drawing 13 of "whereabouts area transmission of a terminal" is a flow chart which shows the subroutine of "whereabouts area transmission of a terminal." If it shifts to this subroutine, the whereabouts area transmitting flag of a terminal is turned on at step S210. If it passes through step S210, it will return to the normal mode. Thereby, in a portable telephone 62, when remote control data are received, since the whereabouts area transmitting flag of a terminal stands, the identification code of the base station 56 where current and a portable telephone 62 are linked is transmitted to its own personal computer 53. Thereby, in a personal computer 53 side, it can recognize that a portable telephone 62 is in the communications area of a base station 56. Moreover, it informs a net control station

57 that the whereabouts area of the base station 56 where current and a portable telephone 62 are linked is transmitted to its own personal computer 53, and you may make it a net control station 57 transmit the whereabouts area of the base station 56 where the portable telephone 62 is linked to the personal computer 53 in response. The location of the base station 56 which has jurisdiction [ portable telephone / 62 ] can become clear by this, and the near range of the portable telephone 62 which this lost (or theft) can also give aim. Therefore, it becomes easy in comparison to find the portable telephone 62 lost (or theft).

[0051] As mentioned above, in the 2nd example, when the owner has noticed loss or the theft of a portable telephone 62, the factor which becomes disadvantageous to the owner of a portable telephone 62 can be prevented by performing the positive security activity (namely, transmission of remote control data) by the owner. Those who acquired when personal digital assistant equipment itself was incidentally lost in the former, or when a theft was suited are able to use the personal digital assistant equipment as it is, and although the payment duty had arisen to the owner in spite of having not used the pocketbook claim of phonecall charges etc., when an owner had not noticed, this fault is cancelable by performing security processing like this example. moreover, even when the communication link of the personal digital assistant equipment which the owner lost through the entrepreneur who notices loss or a theft and forms the public (or dedication) communication network is made impossible Although there was fault that it will not be able to be known by those who acquired an owner's data memorized by personal digital assistant equipment, or the data could not be collected, this fault is cancelable by performing security processing like this example.

[0052] The 3rd example of this invention, next the 3rd example of this invention are explained. Since the positive security activity (transmission of remote control data) by the owner is not performed when an owner does not notice loss or the theft of a portable telephone, possibility by the 3rd person of being used is high. Then, such even case, the control which can perform security processing is automatically explained as the 3rd example. The configuration of the network system of this example and the hard configuration of a portable telephone are the same as that of the 2nd example, and omit illustration. Since the software sides which perform security processing differ, the contents of processing are explained. In addition to said example, the portable telephone of this example realizes the function of an incorrect input information means further.

A. Password configuration-routine drawing 14 by the owner is a flow chart which shows the password configuration routine by the owner. First, in step S250, if a portable telephone comes to hand, an owner will set up a password to a portable telephone, before he begins to use (that is, registration of a password). If this password is not entered in using a portable telephone, it is a kind of key which does

not operate. Moreover, the count of a retry to the incorrect input of a password is set as 3 times. Furthermore, in order to prevent the improper use by the 3rd person, security actuation when there are three incorrect inputs or more of a password is set up.

[0053] Subsequently, a password is registered into the storage section of relation at step S252. The information on this password relation prepares the substorage section (for example, EEPROM or a flash ROM) rather than is memorized to the usual nonvolatile memory, and is registered into this substorage section. Therefore, even if it turns off the power source of a portable telephone, the contents of registration of the substorage section are held. Subsequently, as correspondence in the case of forgetting a password at step S254, a password is transmitted to a base station and it registers with the net control station through the base station. If it passes through step S254, this routine termination will be carried out.

[0054] By performing this routine, various kinds of security processings shown in drawing 15 are performed with a portable telephone.

B. If it shifts to the manipulation routine of manipulation-routine drawing 15 of a device to a password input, the analysis and the count of the password first entered at step S300 will be performed. As for entering a password, it thinks of the owner of normal, or the 3rd person other than an owner (for example, thing which gathered the portable telephone). Subsequently, the password entered at step S302 distinguishes whether it is in agreement with a registered password. If in agreement, this routine will be ended and it will return to the normal mode. Therefore, the usual communication facility etc. is secured and it enables an owner to use a portable telephone.

[0055] On the other hand, in not being in agreement with a password with the entered registered password, it distinguishes whether it progressed to step S304 and there were three incorrect inputs or more. If an incorrect input is less than 3 times, it will return to step S300, the same loop formation will be repeated and an incorrect input will become 3 times or more, it will escape to step S306 and various kinds of security processings will be performed henceforth. Processing to a set up incorrect input is analyzed at step S306. In detail, in order to analyze the processing to a set up incorrect input, the code is assigned, respectively for every processing "communication facility protection", the "contents display protection of storage", "an owner contact display", "alarm sound generating", "prohibition of power-on", "the contents transmission of storage", and "whereabouts area transmission of a terminal", it branches in the code, and it enters to concrete processing. First, in order to tell that there was an incorrect input of a password at step S307, the predetermined telephone number set up beforehand is connected with. Thereby, it can recognize that the portable telephone 62 is used against its mind. Next, it distinguishes whether the analysis result of the processing to a set up incorrect input is the code of "communication facility protection" at step S308, and it branches to step S310 at the

time of YES, and it performs processing of "communication facility protection." Processing of "communication facility protection" is performed by the subroutine, the contents are the same as said example, and illustration of a subroutine is omitted. The flag against a communication link is turned on by performing processing of "communication facility protection", and thereby, since the flag against a communication link stands when performing processing with reference to a flag, the communication facility of a portable telephone stops. Therefore, even when the owner of a portable telephone loses the portable telephone or suits a theft, the 3rd person. can communicate and fault -- the owner of a portable telephone is burdened with an excessive claim -- can be prevented. If it passes through step S310, it will return to the normal mode. In addition, about other processings, it performs by the subroutine similarly, and the fundamental contents are the same as said example, and illustration of a subroutine is omitted. It progresses to step S312 at step S308 at the time of NO.

[0056] At step S312, it distinguishes whether the analysis result of the processing to a set up incorrect input is the code of "the contents display protection of storage", and it branches to step S314 at the time of YES, and it performs processing of "the contents display protection of storage." It progresses to step S16 at step S312 at the time of NO. By performing processing of "the contents display protection of storage", access to a user storage area (an owner's private data and due to occupational cases secret data are memorized) is forbidden. Moreover, you may make it clear the contents of storage. Therefore, even if it can obtain only meaningless data even if the control signal which chooses the corresponding user storage area always serves as a disable and the 3rd person accesses, when there are three incorrect inputs or more of a password, but an owner's private data and due to occupational cases secret data are memorized, it can prevent it being published by the 3rd person or being abused. If it passes through step S314, it will return to the normal mode.

[0057] At step S316, it distinguishes whether the analysis result of the processing to a set up incorrect input is the code of an "owner contact display", and it branches to step S318 at the time of YES, and it performs processing of an "owner contact display." It progresses to step S320 at step S316 at the time of NO. By performing processing of an "owner contact display", the display of a display turns on and an owner contact as shown in drawing 9 is displayed. Therefore, when it loses by mislaying of a portable telephone etc., it enables the person who acquired the portable telephone 62 to the owner to connect by issuing this display. If it passes through step S318, it will return to the normal mode.

[0058] At step S320, it distinguishes whether the analysis result of the processing to a set up incorrect input is the code of "alarm sound generating", and it branches to step S322 at the time of YES, and it performs processing of "alarm sound generating." It progresses to step S323 at step S320 at the time of NO. By performing processing of "alarm sound generating", the flag of alarm sound generating turns on, an alarm

sound occurs from a portable telephone, and a perimeter is told. ** which can also notice the portable telephone which hears it as a result, for example, an alarm sound, and has the 3rd person in a loss location (for example, on the street) If it passes through step S322, it will return to the normal mode.

[0059] At step S324, it distinguishes whether the analysis result of the processing to a set up incorrect input is a code "against power-on", and it branches to step S326 at the time of YES, and it performs processing "against power-on." It progresses to step S328 at step S324 at the time of NO. Even if it makes it a manual and turns ON the switch of a portable telephone by performing processing "against power-on", the microcomputer of a control section checks a power-on prohibition flag in a power-on sequence, and changes to OFF immediately. Therefore, it can change into the condition that it cannot be immediately used even if a portable telephone is in a theft, and the 3rd person can communicate and fault -- the owner of a portable telephone is burdened with an excessive claim -- can be prevented. If it passes through step S326, it will return to the normal mode.

[0060] At step S328, it distinguishes whether the analysis result of the processing to a set up incorrect input is the code of "the contents transmission of storage", and it branches to step S330 at the time of YES, and it performs processing of "the contents transmission of storage." It progresses to step S332 at step S328 at the time of NO. By performing processing of "the contents transmission of storage", the contents of storage of a portable telephone can be copied or transmitted to the storage (for example, a floppy disk or a hard disk) of a personal computer from a portable telephone, data without backup files, such as an individual scheduler, an individual address book, etc., etc. can be easily copied or transmitted to the storage of their own personal computer from a portable telephone, and loss of precious data can be prevented. If it passes through step S330, it will return to the normal mode.

[0061] At step S332, it distinguishes whether the analysis result of the processing to a set up incorrect input is the code of "whereabouts area transmission of a terminal", and it branches to step S334 at the time of YES, and it performs processing of "whereabouts area transmission of a terminal." A system is turned off at step S332 at the time of NO, and it returns to the normal mode (return). By performing processing of "whereabouts area transmission of a terminal", the whereabouts area of the base station connected to the public/leased line network is transmitted to its own personal computer through the public/leased line network with a portable telephone. Thereby, the location of the base station which has jurisdiction [ portable telephone ] becomes clear. If it passes through step S334, it will return to the normal mode. in the 3rd example, things other than an owner gather a portable telephone as mentioned above, or it is ****** -- if the input of the password by which it was going to use the portable telephone and it was mistaken is repeated 3 times or more when it **, various kinds of security processings mentioned above will be performed like the case

where an owner receives remote control data according to the value set up beforehand. Therefore, the same effectiveness as said 2nd example can be acquired.

[0062] In addition, each security processing of "communication facility protection", the "contents display protection of storage", "an owner contact display", "alarm sound generating", "prohibition of power-on", the "contents transmission of storage", and "whereabouts area transmission of a terminal" may perform all automatically, or it may be made to perform any one of these security processings (one [ or ] or more) automatically. Moreover, it is good as for a method of telling that used the sending circuit for coincidence and the incorrect input was made by other persons to the owner. If it is made such, the efficiency of the security to a portable telephone can be raised further. Although the 2nd and 3rd example of the above makes the portable telephone the example as security to personal digital assistant equipment, it is possible to be unable to restrict to a portable telephone, and to be able to apply also to a pocket mold computer (small computer of a tele terminal mold or a PAMUTO top mold) or a pager, for example, to acquire the same effectiveness.

[0063] The 4th example of this invention, next the 4th example of this invention are explained. This example is an example which applied personal digital assistant equipment to the pager equipped with the improper use prevention function.

A. A pager is spreading through the general background of this example widely as versatility, portable ****, and simple and economical mobile means of communications by the generalization of service to use in an individual unit, the miniaturization by technological innovation, lightweight-izing, and multi-functionalization. By the way, it was deficient in the correspondence means which can respond immediately except the notification in **** and the service firm which uses in fact also from the cases where an owner encountered the expectation **** situations, such as loss or a theft, having also increased in number as the pager spread as simple and convenient mobile means of communications. moreover, even if the 3rd person should discover and acquire the pager which carried out loss etc. An owner's name, a contact, etc. are told to an acquisition person and **** information is not displayed. When the worst, could see the message of addressing to an owner individual memorized inside the pager, it was received, and there was a danger that the problem in connection with trust of individuals, such as an owner's privacy and secret leakage, such as improper use of the telephone number, would occur.

[0064] B. The block diagram 16 of a pager is a block diagram which constitutes the electronic circuitry inside the body of a pager 100. In drawing 16 , a pager 100 is roughly divided and is constituted by CPU101, an antenna 102, the RF receive section 103, the decoder section 104, ID-ROM105, ROM106, the key input section 107, a display buffer 108, a display 109, RAM110, the loudspeaker driver 111, a loudspeaker 112, the vibrator driver 113, vibrator 114, the LED driver 115, and LED116. CPU (functional limit means)101 controls each circuit, and realizes a function required for

security processing. The RF receive section 103 restores to the electric wave received with the antenna 102, and outputs to the decoder section 104. ID-ROM105 sends out a frame, the address, etc. which memorized a frame, the address, etc. which are assigned to the pager 100 concerned according to the individual, and have been memorized under control of the decoder section 104 to the decoder section 104. The decoder section 104 outputs a coincidence signal to CPU101, when the input signal which was received in the RF receive section 103 and to which it restored is collated with the data from ID-ROM105 and the input signal is sent to self. An antenna 102, the RF receive section 103, and the decoder section 104 constitute a specific signal detection means.

[0065] The key input section 107 consists of a keyboard part which consists of alphanumeric keys, a function key, etc., and various switch parts, if a certain input is made about a keyboard part, it is processed by CPU101 and RAM110 can be made it is not only to display on the display (specific information display means) 109 equipped with the liquid crystal display panel through the display buffer 108 including the circuit which makes a liquid crystal panel drive as a specific message, but to memorize it. In addition, if a display 109 is a dot display, the display with the kanji is also possible for it. Moreover, various switch parts consist of reset switches operated when stopping generating of the mode circuit changing switch and ringing tone which change the mode between the singing mode in which ringing tone is generated when a call is received, and the silent mode which does not generate ringing tone.

[0066] The LED driver 115 drives LED116 in response to the control signal from CPU101. LED116 is driven to the LED driver 115, blinks or lights up, and performs reception information. The loudspeaker driver 111 drives a loudspeaker 112 in response to the control signal from CPU101. A loudspeaker 112 is driven by the loudspeaker driver 111, and generates ringing tone. The vibrator driver 113 drives vibrator 114 in response to the control signal from CPU101. Vibrator 114 is rocking equipment which drives by the vibrator driver 113 and vibrates, and tells reception by vibration. While specific messages, such as a company name of a service firm, the address, and the telephone number, are beforehand memorized by ROM (specific information storage means)106, the program of security processing is memorized by everything but the message reception performed by CPU. In addition, at the time of specific signal reception, when the specific message data is not memorized by RAM110, it restricts, and it is displayed on a display 109.

[0067] RAM110 consists of specific receiving area SM which memorizes the receipt information area CM which mainly memorizes the past received data etc., and the created specific message. Drawing 17 is drawing showing the register configuration of RAM110. In drawing 17 , a buffer register BR is a register with which the received data sent to CPU101 from the decoder section 104 are once set. It is stood to the area under it at the times, such as generating of ringing tone, and is stood at the time of

generating of the ringing tone in the reset flag RS 1 taken down by pushing a reset button, and a specific signal. The display flag D set when the received message etc. is displayed on the reset flag RS 2 taken down to pushing a reset button, and the display 109 It was stood at the time of the information flag A set while performing reception information by LED116 grade, and singing mode, and the pointer P which specifies each line of the mode flag MF taken down at the time of silent mode and receipt information CM is arranged. The work area W is roughly divided into two area CM, i.e., receipt information area, and the specific receiving area SM. The receipt information area CM is equipped with the receipt time area RT clocked by the telephone number area TN which operates when the usual signal is received, and message areas MA and CPU101. On the other hand, the specific receiving area SM is equipped with the specific message area TA by which call appearance is carried out, the specific signal receipt time area RTS, etc. only when a specific signal is received.

[0068] C. The usual actuation about this security actuation this pager 100 of a pager is the same as that of the pager which has generally spread. Drawing 18 is a flow chart which shows security processing of a pager 100, and is a thing about the case which encountered the situation where an owner did not expect [ theft / loss or ] the pager 100 concerned. When the situation where an owner does not expect [ theft / loss or ] a pager 100 is encountered, a power source shall already turn on a pager 100 at step S400, and it shall be in the condition of the waiting for arrival of the mail. Subsequently, if it progresses to step S402 and an owner transmits a specific signal (for example, signal which orders activation of security processing) to a pager 100 from the exterior using a dial-up line, in the pager 100 concerned, in response to this specific signal, a message will be received in a specific signal with an antenna 102, and it will get over in the RF receive section 103. Subsequently, the signal to which it restored in the decoder section 104 at step S404 is collated by ID-ROM105, and it distinguishes whether it is in agreement with ID specification code beforehand memorized by ID-ROM105. If not in agreement, it returns to step S400 and a loop formation is repeated, and if in agreement, it will escape to step S406. At this time, the signal which shows that it was in agreement from the decoder section 104 to CPU101 is outputted.

[0069] At step S406, the following processing instructions are outputted as security processing.

** a halt of the input function by the key input section 107 -- even if it is going to input the instruction of the 3rd person operating the key input section 107, and displaying data on a display 109 by this, a key input is impossible at all and improper use is prevented.

** a halt of the reception function of the usual signal from the decoder section 104 -- it becomes impossible to receive a received message etc. and improper use is prevented by this.

** starting of an information function -- the LED driver 115 drives by this and reception of a specific signal is reported by LED116. Moreover, a loudspeaker 112 drives by the loudspeaker driver 111, and reception of a specific signal is reported. Furthermore, vibrator 114 drives by the vibrator driver 113, and reception of a specific signal is transmitted by vibration.

[0070] ** a halt of the receiving code output function to RAM110 -- it is lost that the message which storage of the receiving code by RAM110 was not completed, for example, was sent towards the owner by this from others becomes clear to the 3rd person who acquired the pager 100.

** the display of a specific message -- the instruction which displays the specific message memorized beforehand on a display 109 is outputted to RAM110 by this. In addition, when the specific message is not memorized by RAM110, the instruction which displays specific messages, such as a company name of a service firm memorized beforehand, the address, and the telephone number, is outputted to ROM106. Subsequently, it progresses to step S408 and a specific message is displayed on a display 109. A routine will be ended if it passes through step S408. The pager 100 which finally received the specific signal displays a specific message as been in the condition of step S408, for example, shown in drawing 19 etc. on a display 109. In the example of drawing 19 , it is the description which tells the name of ********, the address, a contact, etc. to a finder.

[0071] Even if an owner encounters the expectation **** situations, such as loss or a theft, when a pager 100 discovered and acquires the pager which the 3rd person lost by the above actuation, since it is told to an acquisition person and **** information is displayed, the early detection to the 3rd person and return to an owner can be urged to an owner's name, a contact, etc. Moreover, since the display of the message of addressing to an owner individual memorized inside the pager 100 is forbidden or a key input forbids, the message [ owner ] addressed to an individual can be seen, it can be received, or generating of the problem in connection with trust of individuals, such as an owner's privacy and secret leakage, such as improper use of the telephone number, can be prevented beforehand, and improper use of the pager 100 by the 3rd person can be prevented. In addition, although the personal digital assistant equipment of the security processing object in this example is a pager, the terminal of for example, the communication equipment for personal digital assistants or mobile communication equipment can also apply security processing like this example within the limits of the purpose of this invention.

[0072] Although this example is an example which applied personal digital assistant equipment to PHP, as for this invention, it is needless to say that it is broadly applicable not only to PHP but other personal digital assistant equipments (for example, cordless telephone machine for home use). Moreover, not only the example of the above-mentioned example but other approaches may be used for the method of

checking the same possession nature between telephone 1 and PHP2. For example, the personal identification number for protection corresponding to each protection processing may be prepared, the same owner and the contents of protection processing may be transmitted to coincidence, and may be checked, and a personal identification number and the contents of control may be added to the special ID code for carrying out protection processing. Furthermore, it cannot be overemphasized that what kind of thing is sufficient as the class and the number of each part material which constitutes equipment, the control approach, etc. It is good to perform the same protection processing as this invention by the remote control as for a method of ****** by there being nothing from telephone 1 by making this invention into an expansive gestalt, for example, inputting a predetermined personal identification number etc. even from the public telephone which it is usually also in where in case of emergency.

[0073]

[Effect of the Invention] According to this invention, the following effectiveness can be acquired.

(1) Since the protection processing which eliminates that the owner of personal digital assistant equipment becomes disadvantageous with the protection processing means by the side of personal digital assistant equipment by the owner's inputting a remote command from the exterior, and carrying out the remote control of the personal digital assistant equipment is performing when personal digital assistant equipment is lost, many problems which produce when personal digital assistant equipment is lost by the command from the outside, even if it loses personal digital assistant equipment are appropriately clearable.

(2) That is, while being able to protect the data inside personal digital assistant equipment easily, the fault of it being used for others and charged can be prevented.

(3) The situation which an acquisition person specifically says telephones freely can be prevented, and it can suppress being turned to the contractor of personal digital assistant equipment about the claim of phonecall charges to the minimum.

(4) consequently, in spite of not using it, the fault of avoiding the situation without payment trap ****** where there is nothing, using a tariff for others, and being charged can be prevented.

(5) When the owner has noticed loss or the theft of personal digital assistant equipment, the factor which becomes disadvantageous to the owner of personal digital assistant equipment can be prevented by performing the positive security activity (for example, transmission of remote control data) by the owner. That is, it can protect about the contents of storage of personal digital assistant equipment, and use, being able to protect.

(6) When the owner has noticed loss or the theft of personal digital assistant equipment, an owner's data memorized by personal digital assistant equipment

through the entrepreneur who forms the public (or dedication) communication network can be collected.

(7) If it distinguishes whether it is the no which has a specific signal in the received signal and a specific signal is detected, since security processing which restricts the function of the personal digital assistant equipment will be performed When the situation which is not expected between an owner and personal digital assistant equipment occurs (for example, loss, a theft), by transmitting a specific signal using a dial-up line from the exterior, communication facility can be restricted and the danger of being abused for the 3rd person can be abolished.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the network configuration Fig. of the 1st example of the personal digital assistant equipment concerning this invention.

[Drawing 2] It is the block diagram showing the detailed configuration of PHP of this example.

[Drawing 3] It is the network configuration Fig. of the 2nd example of the personal digital assistant equipment concerning this invention.

[Drawing 4] It is the flow chart which shows the control routine of security processing of this example.

[Drawing 5] It is the flow chart which shows the manipulation routine of the remote control data in the personal digital assistant of this example.

[Drawing 6] It is the flow chart which shows the subroutine of communication facility protection of this example.

[Drawing 7] It is the flow chart which shows the subroutine of the contents display protection of storage of this example.

[Drawing 8] It is the flow chart which shows the subroutine of an owner contact display of this example.

[Drawing 9] It is drawing showing an example of an owner contact display of this example.

[Drawing 10] It is the flow chart which shows the subroutine of alarm sound generating of this example.

[Drawing 11] It is the flow chart which shows the subroutine against [ of this example ]

power-on.

[Drawing 12] It is the flow chart which shows the subroutine of the contents transmission of storage of this example.

[Drawing 13] It is the flow chart which shows the subroutine of whereabouts area transmission of the terminal of this example.

[Drawing 14] It is the flow chart which shows the password configuration routine of the 3rd example of the personal digital assistant equipment concerning this invention.

[Drawing 15] It is the flow chart which shows the manipulation routine of a device to the password input of this example.

[Drawing 16] It is the block diagram showing the electronic circuitry inside the body of the pager of the 4th example of the personal digital assistant equipment concerning this invention.

[Drawing 17] It is drawing showing the register configuration of RAM of this example.

[Drawing 18] It is the flow chart which shows security processing of the pager of this example.

[Drawing 19] It is drawing showing the example of a display of the specific message of this example.

[Description of Notations]

1 Telephone

1b Key stroke section

2 PHP (Portable Cordless Handset Telephone)

3 Communication Line of Cable

4 Relay Center

5 Radio Circuit

11 Control Section (Protection Processing Means, Coincidence Command Means)

14 Key Input Section (Specific Data Specification Means)

15 Display

17 Memory

22 Radio-frequency Head

23 Modem

24 TDMA Signal-Processing Section

25 Speech Codec

26 PCM Codec

31 Receive Section (Receiving Means)

32 Transmitting Section

53 Personal Computer

57 Net Control Station

62 Portable Telephone (Means of Communications, Actuation Data Recognition Means, Security Means, Password Analysis Means, Incorrect Input Information Means)

100 Pager (Personal Digital Assistant Equipment)

101 CPU (Functional Limit Means)
103 RF Receive Section
104 Decoder Section
105 ID-ROM
106 ROM (Specific Information Storage Means)
107 Key Input Section
109 Display
110 RAM
114 Display (Specific Information Display Means)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－193865

(43)公開日　平成７年(1995)７月28日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | 技術表示箇所 |
|---|---|---|---|---|
| Ｈ０４Ｑ　7/38 | | | | |
| Ｈ０４Ｍ　1/00 | Ｎ | | | |
| | | 7605－5Ｋ | Ｈ０４Ｂ　7/ 26　１０９　Ｒ | |

審査請求　未請求　請求項の数15　ＦＤ　（全 19 頁）

(21)出願番号　特願平6－170095

(22)出願日　平成６年(1994)６月28日

(31)優先権主張番号　特願平5－252192
(32)優先日　平５(1993)９月13日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平5－289448
(32)優先日　平５(1993)11月18日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000001443
カシオ計算機株式会社
東京都新宿区西新宿２丁目６番１号
(72)発明者　長谷川　勉
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(72)発明者　杉尾　直昭
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(72)発明者　守屋　孝司
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

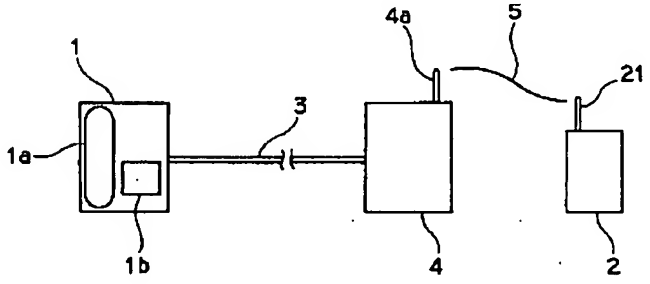
最終頁に続く

(54)【発明の名称】　携帯端末装置およびそのセキュリティ方法

(57)【要約】

【目的】　紛失しても内部データの保護が可能で、かつ他人に使用されて課金されるという不具合を防止できる携帯端末装置およびそのセキュリティ方法を提供する。

【構成】　ＰＨＰ２を紛失した場合、その所有者は電話機１のキー操作部１ｂから指令を入力してＰＨＰ２にリモート操作データを送信する。ＰＨＰ２側ではリモート操作データを受信し、受信したリモート操作データに基づき内部の保護処理手段によりＰＨＰ２の所有者が不利になることを排除する保護処理を実行する。保護処理としては、例えばＰＨＰ２を使用して電話をかけようとするとき、予め記憶されたＰＨＰ２の所有者の連絡先の電話番号の所に全てつながって他にはかけれないようにしたり、ＰＨＰ２の所有者のＩＤデータ等の電話をかけるうえで必要となるデータを全て消去して電話をかけられないようにしたり、あるいは他人に見られると困るようなＰＨＰ２の所有者に関連する特定のデータを消去する処理を行う。



【特許請求の範囲】
【請求項１】　外部より通信回線を介してリモート操作データを受信し、
受信したリモート操作データの内容を解析し、
この解析結果に基づいて携帯端末装置の所有者が不利になることを排除する所定の保護処理を行うことを特徴とする携帯端末装置のセキュリティ方法。
【請求項２】　外部より通信回線を介して入力されたリモート操作データに基づいて、携帯端末装置の所有者が不利になることを排除する所定の保護処理を行う保護処理手段を設けたことを特徴とする携帯端末装置。
【請求項３】　前記保護処理手段は、外部より通信回線を介して入力された暗証番号の一致が確認された後に、前記所定の保護処理を開始することを特徴とする請求項２記載の携帯端末装置。
【請求項４】　前記保護処理手段は、
Ａ．携帯端末装置を使用すると、予め記憶された連絡先につながるようにする保護処理、
Ｂ．携帯端末装置の使用を禁止する保護処理、
Ｃ．携帯端末装置の内部データの表示を禁止する保護処理、
のうちの少なくとも１つ以上を実行することを特徴とする請求項２又は３記載の携帯端末装置。
【請求項５】　前記携帯端末装置に、他人に見られると困るような携帯端末装置の所有者に関連する内部データを特定データとして予め指定可能な特定データ指定手段を、さらに設けたことを特徴とする請求項４記載の携帯端末装置。
【請求項６】　データ通信可能な通信手段と、
送信されてきたデータを解析して、本端末へのリモート操作データであることを認識する操作データ認識手段と、
前記リモート操作データにより本端末に対して所定のセキュリティ処理を実行するセキュリティ手段と、を備えたことを特徴とする携帯端末装置。
【請求項７】　前記セキュリティ手段は、受信したリモート操作データにより、
ａ．正常な立上げシーケンスをとっても、システムが起動しないプロテクト処理
ｂ．携帯端末装置に内蔵されている記憶手段の内容を外部に出力しないプロテクト処理
ｃ．警告音を継続又は断続的に発生するアラーム発生処理
ｄ．携帯端末装置の概略の所在地を所有者に知らせるデータ送信処理
ｅ．携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理
ｆ．携帯端末装置に内蔵されている記憶手段の内容を消去するプロテクト処理
のうちの全てあるいは１つ以上のセキュリティ処理の少なくとも何れかを実行することを特徴とする請求項６記載の携帯端末装置。
【請求項８】　パスワードを入力するパスワード入力手段と、
入力されたパスワードを解析するパスワード解析手段と、を備え、
前記セキュリティ手段は、パスワードの誤入力が所定の設定回数あった場合、前記ａ～ｆのプロテクト処理のうちの全てあるいは１つ以上のセキュリティ処理の少なくとも何れかを実行することを特徴とする請求項７記載の携帯端末装置。
【請求項９】　データ通信可能な通信手段と、
パスワードを入力するパスワード入力手段と、
入力されたパスワードを解析するパスワード解析手段と、
パスワードの誤入力が所定回数あった場合、
ａ．携帯端末装置の概略の所在地を所有者に知らせるデータ送信処理
ｂ．携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理
のうちの全てあるいは１つ以上の所定の少なくとも何れかを実行することを特徴とする携帯端末装置。
【請求項１０】　所有者にパスワードの誤入力があったことを知らせる誤入力報知手段を備えていることを特徴とする請求項８又は９記載の携帯端末装置。
【請求項１１】　呼出とともにメッセージも送られてきた場合に、このメッセージも受信し、
受信した信号に特定の信号がある否かを判別し、
この特定信号を検出すると、当該携帯端末装置の機能を制限するセキュリティ処理を行うことを特徴とする携帯端末装置のセキュリティ方法。
【請求項１２】　呼出とともにメッセージも送られてきた場合に、このメッセージも受信可能なメッセージ受信機能付きの携帯端末装置において、
前記受信した信号のうち、特定の信号を検出する特定信号検出手段と、
この特定信号検出手段によって前記特定信号が検出されると、当該携帯端末装置の機能を制限する機能制限手段と、を設けたことを特徴とする携帯端末装置。
【請求項１３】　前記機能制限手段は、
ａ．キー入力による入力機能の停止
ｂ．通常信号の受信機能の停止
ｃ．報知機能の始動
ｄ．受信コード出力機能の停止
ｅ．特定メッセージの表示
のプロテクト処理のうちの全てあるいは１つ以上のセキュリティ処理の少なくとも何れかを実行することを特徴とする請求項１２記載の携帯端末装置。
【請求項１４】　特定の情報を記憶する特定情報記憶手段と

前記特定信号検出手段によって前記特定信号が検出されると、この特定情報記憶手段に記憶された特定の情報を表示する特定情報表示手段と、を備えたことを特徴とする請求項１２記載の携帯端末装置。

【請求項１５】　前記特定情報記憶手段は、携帯端末装置の利用しているサービス会社、携帯端末装置の所有者の氏名、住所、電話番号等の連絡先を伝える内容を記憶していることを特徴とする請求項１４記載の携帯端末装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、携帯端末装置およびそのセキュリティ方法に係り、詳しくは、リモート操作により外部から携帯端末装置本体の内部制御を行うことを可能にした携帯端末装置、および携帯端末装置の紛失や盗難に対して所有者の不利益を防止可能なセキュリティ方法に関する。

【０００２】

【従来の技術】現在の携帯端末装置の典型的なものとしては、ディジタル無線携帯端末装置が知られており、例えばＰＨＰ（Personal Handy Phone）、ＰＤＡ（Personal Digital Assistant）等がある。ＰＨＰ等は、屋外に設置された基地局を介して公衆回線網に接続されるものであり、屋外に持ち出すことにより、通信範囲を広げることができる。

【０００３】

【発明が解決しようとする課題】ところで、従来の携帯端末装置にあっては、携帯端末装置自体を屋外で紛失したような場合、例えば他人がその紛失した携帯端末装置を取得しても、そのまま使用することが可能であり、通話料金の請求については携帯端末装置の契約者に回されるケースが考えられ、使用していないにもかかわらず料金を支払う必要があるという欠点があった。また、仮に公衆通信のネットを形成している事業者（例えば、いわゆるＮＴＴ、いわゆる第２電電等）側を通して紛失した携帯端末装置を使えないようにしたとしても、電話の通話機能が使用できなくなるだけで、携帯端末装置が所有者の手に戻ってくるわけではないし、携帯端末装置内部の重要なデータ（例えば、個人の電話番号データ）について、他人に知られる可能性があるという欠点があった。

【０００４】そこで本発明は、紛失した場合の不具合を防止できる携帯端末装置および所有者の不利益を防止可能なセキュリティ方法を提供することを目的としている。

【０００５】

【課題を解決するための手段】上記目的達成のため、請求項１記載の発明による携帯端末装置のセキュリティ方法は、外部より通信回線を介してリモート操作データを受信し、受信したリモート操作データの内容を解析しこの解析結果に基づいて携帯端末装置の所有者が不利になることを排除する所定の保護処理を行うことを特徴とする。請求項２記載の携帯端末装置は、外部より通信回線を介して入力されたリモート操作データに基づいて、、携帯端末装置の所有者が不利になることを排除する所定の保護処理を行う保護処理手段を設けたことを特徴とする。

【０００６】好ましい態様として、例えば請求項３記載のように、前記保護処理手段は、外部より通信回線を介して入力された暗証番号の一致が確認された後に、前記所定の保護処理を開始してもよい。また、例えば請求項４記載のように、前記保護処理手段は、

Ａ．携帯端末装置を使用すると、予め記憶された連絡先につながるようにする保護処理、

Ｂ．携帯端末装置の使用を禁止する保護処理、

Ｃ．携帯端末装置の内部データの表示を禁止する保護処理、

のうちの少なくとも１つ以上を実行するようにしてもよい。例えば請求項５記載のように、前記携帯端末装置に、他人に見られると困るような携帯端末装置の所有者に関連する内部データを特定データとして予め指定可能な特定データ指定手段を、さらに設けてもよい。

【０００７】請求項６記載の携帯端末装置は、データ通信可能な通信手段と、送信されてきたデータを解析して、本端末へのリモート操作データであることを認識する操作データ認識手段と、前記リモート操作データにより本端末に対して所定のセキュリティ処理を実行するセキュリティ手段と、を備えたことを特徴とする。また、例えば請求項７記載のように、前記セキュリティ手段は、受信したリモート操作データにより、

ａ．正常な立上げシーケンスをとっても、システムが起動しないプロテクト処理

ｂ．携帯端末装置に内蔵されている記憶手段の内容を外部に出力しないプロテクト処理

ｃ．警告音を継続又は断続的に発生するアラーム発生処理

ｄ．携帯端末装置の概略の所在地を所有者に知らせるデータ送信処理

ｅ．携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理

ｆ．携帯端末装置に内蔵されている記憶手段の内容を消去するプロテクト処理

のうちの全てあるいは１つ以上のセキュリティ処理の少なくとも何れかを実行するようにしてもよい。

【０００８】例えば請求項８記載のように、パスワードを入力するパスワード入力手段と、入力されたパスワードを解析するパスワード解析手段と、を備え、前記セキュリティ手段は、パスワードの誤入力が所定の設定回数あった場合、前記ａ～ｆのプロテクト処理のうちの全てあるいは１つ以上のセキュリティ処理の少なくとも何れ

かを実行するようにしてもよい。請求項９記載の携帯端末装置は、データ通信可能な通信手段と、パスワードを入力するパスワード入力手段と、入力されたパスワードを解析するパスワード解析手段と、パスワードの誤入力が所定回数あった場合、

ａ．携帯端末装置の概略の所在地を所有者に知らせるデータ送信処理

ｂ．携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理

のうちの全てあるいは１つ以上の所定の少なくとも何れかを実行することを特徴とする。例えば請求項１０記載のように、所有者にパスワードの誤入力があったことを知らせる誤入力報知手段を備えるようにしてもよい。

【０００９】請求項１１記載の携帯端末装置のセキュリティ方法は、呼出とともにメッセージも送られてきた場合に、このメッセージも受信し、受信した信号に特定の信号がある否かを判別し、この特定信号を検出すると、当該携帯端末装置の機能を制限するセキュリティ処理を行うことを特徴とする。請求項１２記載の携帯端末装置は、呼出とともにメッセージも送られてきた場合に、このメッセージも受信可能なメッセージ受信機能付きの携帯端末装置において、前記受信した信号のうち、特定の信号を検出する特定信号検出手段と、この特定信号検出手段によって前記特定信号が検出されると、当該携帯端末装置の機能を制限する機能制限手段と、を設けたことを特徴とする。

【００１０】例えば請求項１３記載のように、前記機能制限手段は、

ａ．キー入力による入力機能の停止

ｂ．通常信号の受信機能の停止

ｃ．報知機能の始動

ｄ．受信コード出力機能の停止

ｅ．特定メッセージの表示

のプロテクト処理のうちの全てあるいは１つ以上のセキュリティ処理の少なくとも何れかを実行するようにしてもよい。例えば請求項１４記載のように、特定の情報を記憶する特定情報記憶手段と、前記特定信号検出手段によって前記特定信号が検出されると、この特定情報記憶手段に記憶された特定の情報を表示する特定情報表示手段と、を備えるようにしてもよい。例えば請求項１５記載のように、前記特定情報記憶手段は、携帯端末装置の利用しているサービス会社、携帯端末装置の所有者の氏名、住所、電話番号等の連絡先を伝える内容を記憶しているようにしてもよい。

【００１１】

【作用】本発明では、携帯端末装置を紛失した場合、その所有者あるいは通信事業者は通信回線を介してリモート操作データを入力し、このリモート操作データに基づいき保護処理手段により携帯端末装置の所有者が不利にならることを排除する保護処理が実行される。保護処理としては、例えば携帯端末装置を使用すると、予め記憶された連絡先につながるようにしたり、携帯端末装置の使用を禁止したり、あるいは携帯端末装置の内部データの表示を禁止したりする処理が行われる。したがって、携帯端末装置を紛失しても所有者あるいは通信事業者からの指令で、携帯端末装置内部のデータの保護が可能で、かつ他人に使用されて課金されるという不具合を防止できる。

【００１２】また、他の請求項記載の発明では、外部より送信されたリモート操作データに基づいて、携帯端末装置における操作および使用に対してプロテクトをかけたり、その所在を所有者に連絡したり、記憶されている所有者データを所有者に回収したり、また、所有者が端末の紛失に気が付かなくても、使用に際しパスワードの誤入力が検出されると、セキュリティ処理が実行される。したがって、携帯端末装置を紛失したり、盗難にあった場合でも、所有者に不利益となる事象を取り除くことができ、また、有用なデータを回収することができる。さらに、他の請求項記載の発明では、受信した信号に特定の信号がある否かを判別し、特定信号が検出されると、その携帯端末装置の機能を制限するようなセキュリティ処理が実行される。したがって、所有者と携帯端末装置との間に予期せぬ事態が発生（例えば、紛失、盗難）した場合、外部より公衆電話回線を用いて特定信号を送信することにより、通信機能を制限でき、第３者に悪用される危険性を無くすことができる。

【００１３】

【実施例】以下、図面を参照して本発明の実施例について説明する。

本発明の第１実施例

図１、図２は本発明に係る携帯端末装置の第１実施例を示す図であり、ＰＨＰ（Personal Handy Phone）に適用した例である。

Ａ．ＰＨＰシステムのネットワーク構成

図１はＰＨＰシステムのネットワーク構成図である。図１において、１は公衆回線網（ＰＳＴＮ、ＩＳＤＮ）に接続された電話機、２は携帯用電話としてのＰＨＰ、３は公衆回線網（ＰＳＴＮ、ＩＳＤＮ）に接続された通信回線、４は中継基地局、５は無線通信回線である。また、４ａは中継基地局のアンテナ、２１はＰＨＰ２のアンテナ（図２参照）である。電話機１は、例えば事務所、家庭内あるいは公衆に設置され、公衆回線網に接続され、例えば市内、市外の各種通話が可能な他に、さらに公衆回線網に接続された中継基地局４から無線通信回線５を介してＰＨＰ２の呼出しおよび相互通話が可能である。中継基地局４は比較的小規模のエリア毎に順次配置され、主にＰＨＰ２に対して無線通信回線５を形成し、ＰＨＰ２と他の電話機との間で通話を可能にするような制御を行う。

【００１４】電話機１には送受話器（ハンドセット）、

ａと、電話番号等の入力およびＰＨＰ２をリモート操作する指令を入力する操作部スイッチ１ｂが配置されている。また、操作部スイッチ１ｂは、例えば１０桁の数字あるいは記号を含む暗証番号を入力することができるようになっている。この場合、ＰＨＰ２から受信暗証番号と予め記憶された所定値とが一致したことを示す後述の一致確認信号が電話機１に送信され、電話機１でこの一致確認信号を受信した場合にのみリモート操作データの入力を受け付ける（例えば、リモート操作データ入力受け付けモードを許可する）ようになっている。

【００１５】Ｂ．ＰＨＰブロック構成

図２はＰＨＰ２の詳細な構成を示すブロック図である。図２において、１１は所定プロトコルに従い装置全体の制御を行なう制御部であり、ＣＰＵ等から構成される。制御部１１はＲＯＭ１２に格納されているマイクロプログラムに従ってデータや演算結果などを一時的に記憶するＲＡＭ１３を使用して音声データ送信処理を含むＰＨＰとしてのディジタルコードレス電話装置の各種の動作を制御する。また、本実施例の場合、制御部（保護処理手段）１１は電話機１から送信されたリモート操作データを受信した場合に、この受信したリモート操作データに基づいて、ＰＨＰ２の所有者が不利になることを排除する所定の保護処理を実行するための制御を行う。

【００１６】保護処理の内容は、次の通りである。

モードＡ：後述の表示部１５に予めメモリ１７に記憶しておいた所有者の電話番号を表示させ、ＰＨＰ２を紛失したとき、仮にその紛失したＰＨＰ２を使用して他人が電話をかけようとするとき、予め記憶されたＰＨＰ２の所有者の連絡先の電話番号の所に全てつながるような保護処理

モードＢ：ＰＨＰ２の所有者のＩＤデータ等の電話をかけるうえで必要となるデータを全て消去し、他人が電話をかけられないようにする保護処理

モードＣ：他人に見られると困るようなＰＨＰ２の所有者に関連する特定のデータを消去する保護処理

モードＡ～モードＣの選択は、電話機１側の操作部スイッチ１ｂを操作することにより行う構成になっている。なお、保護処理の内容は上記例に限るものではなく、ＰＨＰ２の所有者が不利になることを排除するものであれば他の保護内容であってもよい。例えば、モードＢにおいて、ＰＨＰ２の後述するキー入力部１４からの信号を受け付けないようにしたり、モードＣにおいて、特定データの表示をソフト的に禁止してもよい。

【００１７】制御部１１には、テンキーや各種のファンクションキーが設けられたキー入力部１４、発信者番号や時刻、通話時間、通話料金等を表示するＬＣＤ等からなる表示部１５、あらかじめ録音されている応答メッセージを送出し、相手からの用件等を録音するカセットテープまたはＩＣメモリからなる録再回路１６、音声データを含む各種データを記憶するメモリ１７が接続されている。ここで、制御部１１は電話機１から送信された暗証番号を受信した場合に、この受信した暗証番号を予めメモリ１７に記憶されている所定値（暗証番号）と比較し、両者が一致したとき、一致したことを示す一致確認信号を電話機１に送信するような制御を行うとともに、少なくともこの一致確認信号を送信した後に、電話機１から送信されてきたリモート操作データに基づいて前述した各種の保護処理（モードＡ～モードＣ）を開始する。したがって、制御部１１は一致指令手段としての機能を有する。

【００１８】また、キー入力部１４は他人に見られると困るようなＰＨＰ２の所有者に関連するデータを特定データとして予め指定可能な特定データ指定手段としての機能を有している。特定データとしては、例えば個人の家庭の電話番号、取り引き先の電話番号、銀行口座番号等がある。これらの特定データはキー入力部１４を操作して予めメモリ１７に記憶させることができるとともに、これらが特定データである旨を指定する特定データ指定入力が可能で、特定データに指定されると、前述したようにモードＣの保護処理が選択された場合に、制御部１１によりメモリ１７の記憶が消去される。

【００１９】Ｃ．ＰＨＰの送信／受信系統

次に、ＰＨＰ２の送信／受信系統について説明する。ＰＨＰ２は、アンテナ２１からの送受信無線周波数（ＲＦ）周波数帯の信号を受信する若しくはモデム２３によりディジタル変調した音声信号を送受信無線周波数（ＲＦ）に周波数変換してアンテナ２１から空中に放出する高周波部２２と、ＲＦ受信した音声信号をディジタル復調する若しくはＴＤＭＡ信号処理部２４によりＴＤＭＡ処理された音声信号をディジタル変調するモデム２３と、無線周波数を時間分割し、特定の時間帯でバースト状に送受信信号を伝送するＴＤＭＡ（Time Division Multiple Access：時分割多元接続）処理を行なうＴＤＭＡ信号処理部２４と、ディジタル音声信号を圧縮／伸張処理を行なうスピーチコーディック２５と、ディジタル信号をアナログ信号に変換してアンプ２７を介して受話器２８に出力する若しくは送話器２９により入力された音声信号をＰＣＭディジタル信号に符号化して出力するＰＣＭコーディック２６と、スピーカ等からなる受話器２８と、マイク等からなる送話器２９と、リンガを鳴らすリンガ部３０とにより構成されている。

【００２０】上記高周波部２２は、周波数変換処理をするものであり、受信部３１、送信部３２、ＰＬＬシンセサイザ３３、バンドパスフィルタ３４および送信／受信を振り分けるアンテナスイッチ３５から構成される。受信部３１は、アンテナ２１で受信されバンドパスフィルタ３４およびアンテナスイッチ３５を介して入力された高周波信号を、２段のミキサーにより周波数変換し、１．９ＧＨｚから１５０～２５０ＭＨｚの周波数帯の信号にし、さらに１０ＭＨｚ付近の中間周波（ＩＦ）信号

に周波数変換する。送信部３２は、モデム２３から入力されたπ／４シフトＱＰＳＫの変調波をミキサーで１．９ＧＨｚに周波数変換し、アンテナスイッチ３５およびバンドパスフィルタ３４を介してアンテナ２１から輻射する。

【００２１】ＰＬＬシンセサイザ３３は、受信部３１および送信部３２での周波数変換のための局部発振をする。上記モデム２３は、π／４シフトＱＰＳＫの変復調処理をするものであり、受信側では、受信部３１からのＩＦ信号を復調してＩＱ信号に分離し、データ列としてＴＤＭＡ信号処理部２４に転送する。また、送信側では、ＴＤＭＡ信号処理部２４から転送されてきたデータからＩＱ信号を作成してπ／４シフトＱＰＳＫの変調をして送信部３２に出力する。

【００２２】上記ＴＤＭＡ信号処理部２４は、フレーム同期およびスロットのフォーマット処理をする。すなわち、受信側では、モデム２３か送られてくるデータから所定タイミングで自己宛てのスロットのデータを取り出し、スクランブル等を解除して、このスロットのフォーマットから構成データを取り出し、制御データは制御部１１に送り、音声データはスピーチコーディック２５に転送する。送信側では、スピーチコーディック２５から転送されてくる音声データに制御データを付加して送信データを作成し、スクランブル等をかけて所定タイミングで、すなわちフレームの自己割り当てスロットに挿入してモデム２３に送出する。

【００２３】また、ＴＤＭＡ信号処理部２４は、基地局４の間で時間的に重ならないように同一周波数の信号を送受し、相互に通信を行なうように処理するものであり、信号の送受信は基本周期となる一定長のＴＤＭＡフレーム内に割り当てられた一対の時間位置（タイムスロット）を用いて行われる。各局はフレーム内の割り当てられたタイムスロットに信号を送出し、この信号が他の信号に衝突しないようにその時間位置制御（バースト同期制御）を行なう。

【００２４】スピーチコーディック２５は、ディジタルデータの圧縮／伸張処理をする。すなわち、受信側では、ＴＤＭＡ信号処理部２４から送られてきたＡＤＰＣＭ音声信号（４ｂｉｔ×８ｋＨｚ＝３２ｋ bps）をＰＣＭ音声信号（８ｂｉｔ×８ｋＨｚ＝６４ｋ bps）に復号化することにより伸張してＰＣＭコーディック２６に出力する。送信側では、ＰＣＭコーディック２６から送られてきたＰＣＭ音声信号をＡＤＰＣＭ音声信号に符号化することにより圧縮してＴＤＭＡ信号処理部２４に出力する。ＰＣＭコーディック２６は、アナログ／ディジタル変換処理をする。受信側では、スピーチコーディック２５から送られてくるＰＣＭ音声信号をＤ／Ａ変換してアナログ音声信号をアンプ２７に出力してスピーカ２８を駆動する。送信側では、マイク２９から入力されたアナログ音声信号をＡ／Ｄ変換してＰＣＭ音声信号をスピーチコーディック２５に出力する。また、ボリューム／リンガ／トーン信号等の制御を行なう。

【００２５】次に、作用を説明する。

Ｄ．全体の通信動作

電話機１は、例えば事務所、家庭内あるいは公衆に設置され、通信回線３を介して公衆回線網に接続されることより、市内、市外の各種通話が行われる。また、中継基地局４から無線通信回線５を介してＰＨＰ２の呼出しおよび相互通話が行われる。この場合、中継基地局４は比較的小規模のエリア毎に順次多数が配置され、主にＰＨＰ２に対して無線通信回線５を形成し、ＰＨＰ２と他の電話機との間で通話を可能にするような制御が行われる。

【００２６】Ｅ．ＰＨＰの全体動作

本実施例のＰＨＰ２におけるアクセス方式および伝送方式はＴＤＭＡ／ＴＤＤ通信方式を採用しており、時分割で複数の端末と通信し、上り／下りのデータも時分割して同一周波数上に乗せている。すなわち、中継基地局４を介して送信された相手局（例えば、電話機１や他の端末電話装置）からの音声はアンテナ２１を通して高周波部２２によりベースバンド信号に変換されて受信され、受信された音声信号はモデム２３によりディジタル復調されてＴＤＭＡ信号処理部２４に出力される。ＴＤＭＡ信号処理部２４は送信信号に付加された制御信号（搬送波同期、ビット同期、フレーム同期信号）を基に受信したディジタル音声信号が送信時の信号と衝突しないように受信のタイミングを制御するとともに、バースト状に送られてくる信号を元の伝送速度に変換して音声信号を取り出す。ＴＤＭＡ信号処理部２４により取出されたディジタル音声信号はスピーチコーディック２５により伸張され、ＰＣＭコーディック２６によりアナログ音声信号に変換されてアンプ２７を介して受話器２８から放音される。

【００２７】一方、送話器２９から入力された音声信号はＰＣＭコーディック２６によりＰＣＭディジタル信号に符号化され、符号化されたディジタル信号はスピーチコーディック２５によりデータ圧縮されてＴＤＭＡ信号処理部２４に出力される。ＴＤＭＡ信号処理部２４は所定の送信タイミングで信号をバースト状に送信するバースト送信制御を行って送信するバースト信号をモデム２３に出力する。モデム２３に入力された送信信号はここでディジタル変調されて高周波部２２に出力され、高周波部２２で無線周波数に周波数変換されてアンテナ２１を通して空中に放出される。また、制御部１１では、高周波部２２の送信部３２のバースト制御信号入力端子に、送信出力をバースト波にするためのバースト制御信号を出力するとともに、キー入力部１４からのキー操作情報を基にモードの切替えや状態を制御し、制御結果に基づく表示信号を表示部１５に送出したり、ＴＤＭＡ信号処理部２４からの着信を受けた場合にリンガ２９を鳴

らす等の制御を行なう。空中に放出された電波は無線通信回線５を介して中継基地局４のアンテナ４ａによってキャッチされ、中継基地局４において処理された後、通信回線３を介して電話機１に送信され、電話機１で受信される。

【００２８】Ｆ．保護処理動作

次に、本実施例の特徴部分である保護処理動作について説明する。まず、ＰＨＰ２を所有者が紛失した場合、その所有者（すなわち、真の所有者）は電話機１のキー操作部１ｂを操作してＰＨＰ２に電話をかける。ＰＨＰ２に電話がかかると、電話機１とＰＨＰ２との間にデータを送受信可能な相互の通信回線ネットが形成される。このとき、紛失したＰＨＰ２は、例えばそれを取得して所有している者（以下、取得者という）の手元にあるケースが多い。次いで、ＰＨＰ２の所有者はキー操作部１ｂを操作して暗証番号入力モードをセレクトし、所定の暗証番号（例えば、１０桁の番号で「＃１１２２３３４４＃」）を入力する。暗証番号に代えて、例えばＰＨＰ２の所有者のＩＤコードでもよい。

【００２９】暗証番号が入力されると、ＰＨＰ２側では受信した暗証番号を予めメモリ１７に記憶しておいた所定値（例えば、暗証番号と同じ値）と比較し、両者が一致したとき、一致したことを示す一致確認信号を電話機１に送信する。電話機１では、一致確認信号を受信した場合にのみリモート操作データの入力受け付けが可能となる。次いで、ＰＨＰ２の所有者はキー操作部１ｂを操作してリモート操作指令を入力する。ＰＨＰ２側では、このリモート操作指令に対応するリモート操作データに基づいてＰＨＰ２の所有者が不利になることを排除する保護処理の何れか（モードＡ、モードＢあるいはモードＣ）の実行が開始される。なお、制御部１１は前述した一致確認信号を送信した後でなければ、保護処理を開始しない。

【００３０】（ａ）「モードＡ」の選択

例えば、保護処理として「モードＡ」を選択したときには、表示部１５に予めメモリ１７に記憶しておいた所有者の電話番号を表示させ、紛失したＰＨＰ２を使用して他人（取得者）が電話をかけようとした場合に、予め記憶されたＰＨＰ２の所有者の連絡先の電話番号の所に全てつながるような処理が行われる。したがって、取得者が勝手に電話をかけまくるというような事態を防ぐことができ、通話料金の請求についてＰＨＰ２の契約者に回されることを最小限に抑えることができる。その結果、使用していないにもかかわらず料金を支払らわなければないないという事態を避けて、他人に使用されて課金されるという不具合を防止することができる。また、この場合、ＰＨＰ２の所有者の連絡先の電話番号の所に全てつながるから、仮にＰＨＰ２の取得者が電話をしてきたならば、ＰＨＰ２の所有者は取得者に対してＰＨＰ２を返却するように要請することもでき、極めて好都合である。すなわち、真の所有者の手に戻りやすくすることができるから、実際上、真の所有者の手に戻って来ることも有り得る。

【００３１】（ｂ）「モードＢ」の選択

次に、保護処理として例えば「モードＢ」を選択したときには、ＰＨＰ２の所有者のＩＤデータ等の電話をかけるうえで必要となるデータが全て消去され、他人が電話をかけられないようにする保護処理が行われる。したがって、取得者がＰＨＰ２を使用して電話しようと試みても、電話ができず、勝手に電話をかけまくるというような事態を防ぐことができ、上記同様に他人に使用されて課金されるという不具合を防止することができる。

【００３２】（ｃ）「モードＣ」の選択

また、保護処理として例えば「モードＣ」を選択したときには、他人に見られると困るようなＰＨＰ２の真の所有者に関連する特定のデータを消去する保護処理が行われる。ただし、「モードＣ」の選択のみでは、電話機能は許可されている。したがって、予め指定されておいた個人の家庭の電話番号、取り引き先の電話番号、銀行口座番号等が全て消去される。その結果、重要なデータについて、他人に知られなくすることができる。すなわち、重要なデータの保護を図ることができる。このように、電話機１からのリモート操作により、ＰＨＰ２を紛失した場合に生じる諸問題を適切にクリアすることができる。

【００３３】本実施例は携帯端末装置をＰＨＰに適用した例であるが、本発明はＰＨＰに限らず、他の携帯端末装置（例えば、家庭用のコードレス電話機）にも幅広く適用できるのは勿論である。また、電話機１とＰＨＰ２との間の同一所有性を確認する方法は、上記実施例の例に限らず、他の方法を用いてもよい。例えば、各保護処理に対応した保護用の暗証番号を設けて、同一所有者と保護処理内容を同時に転送して確認してもよいし、保護処理をするための特別のＩＤコードに暗証番号と制御内容を付加してもよい。さらに、装置を構成する各部材の種類・個数、制御方法等は、どのようなものでもよいことは言うまでもない。本発明の発展的形態として、例えば電話機１からでなく、緊急の場合には通常どこにでもある公衆電話からでも所定の暗証番号等を入力することにより、リモート操作により、本発明と同様の保護処理を行うことができるようにしてもよい。

【００３４】本発明の第２実施例

次に、本発明の第２実施例について説明する。

Ａ．ネットワークシステムの構成

図３は本発明を適用した携帯端末装置のネットワークシステムを示す図である。図３において、５１は公衆／専用回線網であり、ここでの公衆／専用回線網は一般の電話公衆網である。公衆／専用回線網５１には一般の電話機５２、モデムを介してのパーソナルコンピュータ５３、携帯端末用の複数の基地局５４、５５および網管理

局５７が接続されている。複数の基地局５４～５６には携帯端末がそれぞれ無線を介して接続されている。すなわち、基地局５４は無線を介して携帯型コンピュータ６１に接続され、基地局５５は無線を介して携帯電話機６２に接続され、さらに基地局５６は無線を介してページャ６３に接続されている。携帯型コンピュータ６１としては、例えばテレターミナル型やパームトトップ型の小型コンピュータが用いられる。携帯電話機６２としては、例えばＰＨＰや複数の各社で販売されているもの（例えば、セルラーフォーン）が用いられる。ページャ６３としては、ＮＰ、ＩＰ等のタイプのものが用いられる。網管理局５７は網全体の管理を行うもので、各携帯端末に対しての制御を行う。

【００３５】Ｂ．プロテクト回路の構成

ここで、本実施例では携帯電話機６２にセキュリティ機能を実現するプロテクト装置を付加した例について説明する。ハード的な主要部の構成は前述した第１実施例の図２に示すものと同様であり、その他に本実施例ではプロテクト装置が付加されている。プロテクト装置は所有者より送信されたリモート操作データを受信した場合、このリモート操作データに基づいて携帯電話機６２の所有者に不利益となる要因を削除する所定のセキュリティ処理を実行するための制御や、パスワードの入力・解析処理を実行するための制御を行い、また、誤った入力に対しても設定されたセキュリティ処理を実行するための制御を行う。携帯電話機６２は通信手段、操作データ認識手段、セキュリティ手段、パスワード解析手段の機能を実現する。

【００３６】次に、作用を説明する。

Ｃ．セキュリティ処理のメインルーチン

図４、５はプロテクト装置における保護機能（セキュリティ処理）を実現するメインルーチンを示すフローチャートである。

（ａ）所有者によるプロテクト装置の制御

携帯電話機６２の所有者が、その携帯電話機６２を紛失したり、盗難にあった場合、図４に示すセキュリティ処理の制御ルーチンが実行される。すなわち、ステップＳ１０において、携帯電話機６２の所有者は網管理局５７に対してモデムを介して接続されたパーソナルコンピュータ５３を用いて所有する携帯電話機６２に対して通信を開始すべくリモート操作データを入力する。このとき、携帯電話機６２が無くなったときの状況および内部に記憶されている情報の重要度により送信するリモート操作データの内容を選択する。リモート操作データには制御コードが付加されており、所有者しか知らない暗証番号が含まれている。したがって、第３者が任意に所有者の携帯電話機６２に対してリモート操作データを送ることはできない。これにより、リモート操作の悪用を防止可能である。

【００３７】一方、携帯電話機６２の所有者がパーソナルコンピュータ５３を保有していないような場合、あるいは保有していても網管理局５７に対してモデムを介してアクセスできるシステムになっていないときは、一般の電話機５２（例えば、個人所有の電話機）により音声によって携帯電話機６２の基地局５５にリモート操作データの送信を依頼する。あるいは、電話機５２を使用しプッシュ回線によりリモート操作データを入力する。次いで、ステップＳ１２で携帯電話機６２の所有者が入力したリモート操作データを公衆／専用回線網５１を通して携帯電話機６２の基地局５５に転送する。次いで、ステップＳ１４に進み、携帯電話機６２の基地局５５より無線にてリモート操作データを送信する（データの送信はＴで示す）。このようにしてパーソナルコンピュータ５３より入力されたリモート操作データが公衆／専用回線網５１および網管理局５７を介して携帯電話機６２の基地局５５へ送られ、目的の携帯電話機６２に送信される。なお、携帯電話機６２が双方向通信の機能を有していれば、リンクが確立され、所有者の操作するパーソナルコンピュータ５３へ携帯電話機６２側の受信が確実に行われたことを伝達する。

【００３８】（ｂ）携帯端末におけるリモート操作データの処理

図４の処理が実行され、基地局５５より無線にてリモート操作データが携帯電話機６２に送信されると、図５に示す携帯端末におけるリモート操作データの処理ルーチンが実行される。まず、ステップＳ２０でリモート操作データ（図５ではリモートデータと簡略化する）の受信によりシステムをウェークアップする。これにより、携帯電話機６２では表示部を除いてセキュリティ処理のシステムが起動（例えば、プロテクト装置等が起動）する。次いで、ステップＳ２２で自分（携帯電話機６２）に対してのリモート操作データであるか否かを判別する。これは、例えば暗証番号の一致を含めて判断する。自分へのリモート操作データでないとき、あるいは暗証番号が違っていた場合には、システムをオフし、通常モードへ戻る（リターン）。

【００３９】自分へのリモート操作データであり、かつ暗証番号が一致していた場合にはステップＳ２４に進み、リモート操作データの内容の解析を行う。詳しくは、リモート操作データには「通信機能プロテクト」、「記憶内容表示プロテクト」、「所有者連絡先表示」、「アラーム音発生」、「パワーオン禁止」、「記憶内容送信」、「端末の所在エリア送信」という処理毎にそれぞれコードが割り当てられており、そのコードにより分岐し、具体的な処理に入る。すなわち、ステップＳ２６でリモート操作データの内容の解析結果が「通信機能プロテクト」のコードであるか否かを判別し、ＹＥＳのときはステップＳ２８に分岐して「通信機能プロテクト」の処理を実行する。「通信機能プロテクト」の処理はサブルーチンで後述する。他の処理についても、同様にサ

ブルーチンで後述する。ステップＳ２６でＮＯのときはステップＳ３０に進む。

【００４０】ステップＳ３０では、リモート操作データの内容の解析結果が「記憶内容表示プロテクト」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３２に分岐して「記憶内容表示プロテクト」の処理を実行する。ステップＳ３０でＮＯのときはステップＳ３４に進む。ステップＳ３４では、リモート操作データの内容の解析結果が「所有者連絡先表示」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３６に分岐して「所有者連絡先表示」の処理を実行する。ステップＳ３４でＮＯのときはステップＳ３８に進む。

【００４１】ステップＳ３８では、リモート操作データの内容の解析結果が「アラーム音発生」のコードであるか否かを判別し、ＹＥＳのときはステップＳ４０に分岐して「アラーム音発生」の処理を実行する。ステップＳ３８でＮＯのときはステップＳ４２に進む。ステップＳ４２では、リモート操作データの内容の解析結果が「パワーオン禁止」のコードであるか否かを判別し、ＹＥＳのときはステップＳ４４に分岐して「パワーオン禁止」の処理を実行する。ステップＳ４２でＮＯのときはステップＳ４６に進む。ステップＳ４６では、リモート操作データの内容の解析結果が「記憶内容送信」のコードであるか否かを判別し、ＹＥＳのときはステップＳ４８に分岐して「記憶内容送信」の処理を実行する。ステップＳ４６でＮＯのときはステップＳ５０に進む。ステップＳ５０では、リモート操作データの内容の解析結果が「端末の所在エリア送信」のコードであるか否かを判別し、ＹＥＳのときはステップＳ５２に分岐して「端末の所在エリア送信」の処理を実行する。ステップＳ５０でＮＯのときはシステムをオフし、通常モードへ戻る（リターン）。

【００４２】Ｄ．セキュリティ処理のサブルーチン

次に、リモート操作データの内容の解析結果に基づく、具体的な各プロテクト処理のサブルーチンについて説明する。

①「通信機能プロテクト」のサブルーチン

図６は「通信機能プロテクト」のサブルーチンを示すフローチャートである。このサブルーチンに移行すると、ステップＳ１００で通信禁止のフラグをオンする。これにより、フラグを参照して処理を実行するとき、通信禁止のフラグが立っているから、携帯電話機６２の通信機能が停止する。したがって、携帯電話機６２の所有者が、その携帯電話機６２を紛失したり、盗難にあった場合でも、第３者が通信を行って過大な請求が携帯電話機６２の所有者に課せられる等の不具合を防止することができる。ステップＳ１００を経ると、通常モードへ戻る。

【００４３】②「記憶内容表示プロテクト」のサブルーチン

図７は「記憶内容表示プロテクト」のサブルーチンを示すフローチャートである。このサブルーチンに移行すると、ステップＳ１１０でユーザー記憶エリア選択信号をディスエーブルするラッチをオンする。ステップＳ１１０を経ると、通常モードへ戻る。これにより、ユーザー記憶エリア（所有者のプライベートデータや業務上の機密データを記憶）に対するアクセスが禁止される。したがって、リモート操作データを受信した場合、該当するユーザー記憶エリアを選択する制御信号が常にディスエーブルとなり、仮に第３者がアクセスしても、全て［ＦＦｈ」あるいは「００ｈ」というような意味のないデータしか得ることができなくなる。その結果、所有者のプライベートデータや業務上の機密データが記憶されていた場合であっても、第３者によって公にされたり、悪用されたりするのを防止することができる。また、このときユーザー記憶エリア内のデータを消去するようにしてもよい。これにより、ユーザー記憶エリアをアクセスしても表示されるデータはないので、第３者によって公にされたり、悪用されたりするのを防止することができる。

【００４４】③「所有者連絡先表示」のサブルーチン

図８は「所有者連絡先表示」のサブルーチンを示すフローチャートである。このサブルーチンに移行すると、ステップＳ１２０で表示部の表示をオンする。これにより、表示部による表示が可能になる。次いで、ステップＳ１２２で表示部に、例えば図９に示すような所有者連絡先を表示する。図９は、携帯端末機器を紛失した場合の表示例であり、氏名、住所、電話番号が表示される。携帯電話機６２の置き忘れ等により紛失した場合には、この表示を出すことにより、所有者に対して携帯電話機６２を取得した人が連絡することが可能になる。ただし、ここで表示部の表示をオンしっぱなしにすると、人目につかないうちに携帯電話機６２に内蔵の電池が切れるおそれがあるため、一定時間経過後に自動的に表示を消す処理を行う。

【００４５】すなわち、ステップＳ１２４でタイマーのカウントを行い、ステップＳ１２６で設定時間（例えば、１時間）が経過したか否かを判別する。設定時間が経過していなければステップＳ１２４に戻ってループを繰り返し、設定時間が経過すると、ステップＳ１２８に抜け表示部の表示をオフする。これにより、所有者連絡先の表示が消える。ステップＳ１２８を経ると、通常モードへ戻る。このように一定時間経過後に自動的に表示を消す処理を行うことにより、電池の消耗を防ぎつつ必要な表示を行って、第３者に対する所有者連絡先をアピールすることができる。したがって、例えば携帯電話機６２を取得した人が所有者に連絡することができれば、所有者の手元に返却してもらうことも可能になる。なお、所有者連絡先は、例えば間欠的に表示させたり、あるいは所有者がリモート操作データを送信した後、１回

だけある一定時間表示するようにしてもよい。また、ステップＳ４０の「アラーム音発生」と併用してアラーム音を鳴らすようにしてもよい。そのようにすると、より効果的に第３者に対して所有者連絡先をアピールすることができる。

【００４６】④「アラーム音発生」のサブルーチン

図１０は「アラーム音発生」のサブルーチンを示すフローチャートである。このサブルーチンに移行すると、ステップＳ１５０でアラーム音発生のフラグをオンする。これにより、フラグを参照して処理を実行するとき、アラーム音発生のフラグが立っているから、携帯電話機６２からアラーム音（例えば、スピーカー）が発生し、周囲に知らせることになる。したがって、携帯電話機６２の所有者が、その携帯電話機６２を紛失したり、盗難にあった場合、リモート操作データを送信することにより遠隔的に携帯電話機６２のアラーム音を鳴らすことができ、携帯電話機６２についての異常状態を報知することができる。その結果、例えばアラーム音を聞いて第３者が紛失場所（例えば、路上）にある携帯電話機６２に気付くことも可能なる。ステップＳ１５０を経ると、通常モードへ戻る。

【００４７】⑤「パワーオン禁止」のサブルーチン

図１１は「パワーオン禁止」のサブルーチンを示すフローチャートである。このサブルーチンに移行すると、ステップＳ１６０でパワーオンスイッチをディスエーブルするフラグ（パワーオンスイッチディスエーブルフラグ）をオンする。ステップＳ１６０を経ると、通常モードへ戻る。これにより、携帯電話機６２のパワーオン自体を禁止する命令が実行されることになる。すなわち、リモート操作データを受信した場合、パワーオンスイッチディスエーブルフラグが立っているから、マニュアルにして携帯電話機６２のスイッチをオンにしても、制御部のマイクロコンピュータはパワーオンシーケンスにて本フラグをチェックし、フラグがオンであれば、パワーオン処理を中断し、即座にオフへと遷移する。したがって、携帯電話機６２が盗難にあったような場合、携帯電話機６２が他の者に利用され、回線使用料を使ってもいない所有者に請求される可能性もあるが、本実施例のようにパワーオン処理を中断することにより、盗難にあってもすぐに使用できない状態にすることができ、第３者が通信を行って過大な請求が携帯電話機６２の所有者に課せられる等の不具合を防止することができる。例えば、クレジットカードを紛失した場合、業者に連絡してその使用を停止してもらうシステムになっているが、同様の処理を携帯電話機６２の所有者が即座に実行できることになる。

【００４８】⑥「記憶内容送信」のサブルーチン

図１２は「記憶内容送信」のサブルーチンを示すフローチャートである。このサブルーチンに移行すると、ステップＳ２００で本コマンドを受信した携帯電話機６２は所有者の指定する端末（指定端末は制御コード内に記述されている）との間でリンクを確立する。この場合はモデムにより公衆／専用回線網５１に接続されたパーソナルコンピュータ５３とのリンクを確立することになる。次いで、ステップＳ２０２で携帯電話機６２からパーソナルコンピュータ５３に記憶内容を送信する。ここでの記憶内容とは、個人のスケジューラーや住所録等バックアップファイルを持っていない場合や、出先で入力した業務上のデータ等、回収したいデータが携帯電話機６２に記憶されていたとき、その記憶データをいう。

【００４９】ステップＳ２０２の処理を実行することにより、所有者の指定する端末へアップロードすることが可能になる。次いで、ステップＳ２０４でパーソナルコンピュータ５３が正確に受信したか否かを判別する（パーソナルコンピュータ５３からの受領信号に基づいて）。正確に受信していなければ、ステップＳ２０２に戻って受信ループを繰り返し、正確に受信すると、ステップＳ２０６で記憶内容をクリアする処理を実行することにより、送信したデータをクリアし、通常モードへ戻る。なお、他のデータ保護処理と併用する場合は、ステップＳ２０６のデータクリアは必ずしも必要ではない。これにより、携帯電話機６２からパーソナルコンピュータ５３の記憶媒体（例えば、フロッピィディスク、あるいはハードディスク）に携帯電話機６２の記憶内容が複写あるいは転送され、データがエラー無しに複写あるいは転送されたことを確認して本動作が終了する。したがって、携帯電話機６２が盗難にあった場合、あるいは携帯電話機６２を紛失した場合でも、個人のスケジューラーや住所録等バックアップファイルを持っていないデータや、出先で入力した業務上のデータ等、回収したいデータを携帯電話機６２から簡単に自分のパーソナルコンピュータ５３の記憶媒体に複写あるいは転送することができ、貴重なデータの紛失を防ぐことができる。

【００５０】⑦「端末の所在エリア送信」のサブルーチン

図１３は「端末の所在エリア送信」のサブルーチンを示すフローチャートである。このサブルーチンに移行すると、ステップＳ２１０で端末の所在エリア送信フラグをオンする。ステップＳ２１０を経ると、通常モードへ戻る。これにより、携帯電話機６２ではリモート操作データを受信した場合、端末の所在エリア送信フラグが立っているから、現在、携帯電話機６２がリンクされている基地局５６の識別コードを自分のパーソナルコンピュータ５３に送信する。これにより、パーソナルコンピュータ５３側では、基地局５６の通信エリア内に携帯電話機６２があることを認識できる。また、現在、携帯電話機６２がリンクされている基地局５６の所在エリアを自分のパーソナルコンピュータ５３に送信するように網管理局５７に連絡し、網管理局５７は、これを受けてパーソナルコンピュータ５３に携帯電話機６２がリンクされて

いる基地局５６の所在エリアを送信するようにしてもよい。これにより、携帯電話機６２を管轄する基地局５６の位置が判明し、それにより紛失（あるいは盗難）した携帯電話機６２のおよその範囲も見当をつけることができる。したがって、紛失（あるいは盗難）した携帯電話機６２を見つけることが比較的に容易になる。

【００５１】以上のように第２実施例では、所有者が携帯電話機６２の紛失あるいは盗難に気付いた場合、所有者による積極的なセキュリティ活動（すなわち、リモート操作データの送信）を行うことによって、携帯電話機６２の所有者に不利益となる要因を防止することができる。因みに、従来では携帯端末装置自体を紛失した場合、又は盗難にあった場合、取得した者がその携帯端末装置をそのまま使用することが可能であり、所有者が気付かないときには通話料金等の金銭的な請求は使用していないにもかかわらず、所有者に支払義務が生じていたが、本実施例のようなセキュリティ処理を実行することにより、かかる不具合を解消することができる。また、所有者が紛失又は盗難に気が付き、公衆（あるいは専用）通信ネットワークを形成している事業者を通して紛失した携帯端末装置を通信不可能にした場合でも、携帯端末装置に記憶された所有者のデータを取得した者に知られてしまったり、そのデータを回収することができないという不具合があったが、本実施例のようなセキュリティ処理を実行することにより、かかる不具合を解消することができる。

【００５２】本発明の第３実施例

次に、本発明の第３実施例について説明する。所有者が携帯電話機の紛失あるいは盗難に気付かない場合には、所有者による積極的なセキュリティ活動（リモート操作データの送信）が行われないため、第３者による使用される可能性が高い。そこで、そのような場合でも自動的にセキュリティ処理を実行可能な制御を、第３実施例として説明する。本実施例のネットワークシステムの構成および携帯電話機のハード的な構成は、第２実施例と同様であり、図示を省略する。セキュリティ処理を実行するソフト面が異なるので、その処理内容を説明する。本実施例の携帯電話機は、前記実施例に加えて、さらに誤入力報知手段の機能を実現する。

Ａ．所有者によるパスワード設定ルーチン

図１４は所有者によるパスワード設定ルーチンを示すフローチャートである。まず、ステップＳ２５０において、所有者は携帯電話機を入手すると、使い始める前に携帯電話機に対してパスワードを設定（つまりパスワードの登録）する。このパスワードは携帯電話機を使用するにあたって入力しないと、動作しない一種の鍵である。また、パスワードの誤入力に対するリトライ回数を３回に設定する。さらに、第３者による悪用を防ぐため、パスワードの誤入力が３回以上あった場合のセキュリティ動作の設定をしておく。

【００５３】次いで、ステップＳ２５２でパスワードを関連の記憶部に登録する。本パスワード関連の情報は、通常の不揮発メモリに記憶しておくのではなく、副記憶部（例えば、ＥＥＰＲＯＭあるいはフラッシュＲＯＭ）を設け、この副記憶部に登録される。したがって、携帯電話機の電源をオフしても、副記憶部の登録内容は保持される。次いで、ステップＳ２５４でパスワードを忘れてしまった場合の対応として、パスワードを基地局へ転送し、基地局を通して網管理局に登録しておく。ステップＳ２５４を経ると、本ルーチン終了する。

【００５４】本ルーチンを実行しておくことにより、携帯電話機では図１５に示す各種のセキュリティ処理が実行される。

Ｂ．パスワード入力に対する機器の処理ルーチン

図１５の処理ルーチンに移行すると、まずステップＳ３００で入力されたパスワードの解析およびカウントを行う。パスワードを入力するのは正規の所有者あるいは所有者以外の第３者（例えば、携帯電話機を拾ったもの）が考えられる。次いで、ステップＳ３０２で入力されたパスワードが登録済みのパスワードと一致するか否かを判別する。一致していれば、本ルーチンを終了して通常モードへ戻る。したがって、通常の通信機能等が確保され、所有者が携帯電話機を使用することが可能になる。

【００５５】一方、入力されたパスワードが登録済みのパスワードと一致しない場合には、ステップＳ３０４に進んで誤入力が３回以上あったか否かを判別する。誤入力が３回未満であれば、ステップＳ３００に戻って同様のループを繰り返し、誤入力が３回以上になると、ステップＳ３０６に抜け、以後、各種のセキュリティ処理を行う。ステップＳ３０６では設定済み誤入力に対する処理の解析を行う。詳しくは、設定済み誤入力に対する処理を解析するには、「通信機能プロテクト」、「記憶内容表示プロテクト」、「所有者連絡先表示」、「アラーム音発生」、「パワーオン禁止」、「記憶内容送信」、「端末の所在エリア送信」という処理毎にそれぞれコードが割り当てられており、そのコードにより分岐し、具体的な処理に入る。まず、ステップＳ３０７でパスワードの誤入力があったことを知らせるために、予め設定してある所定電話番号に連絡する。これにより、自分の意と反して携帯電話機６２が使用されていることを認識することができる。次に、ステップＳ３０８で設定済み誤入力に対する処理の解析結果が「通信機能プロテクト」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３１０に分岐して「通信機能プロテクト」の処理を実行する。「通信機能プロテクト」の処理はサブルーチンで実行され、その内容は前記実施例と同様であり、サブルーチンの図示は省略する。「通信機能プロテクト」の処理を実行することにより、通信禁止のフラグがオンになり、これにより、フラグを参照して処理を実行するとき、通信禁止のフラグが立っているから、携帯電話機

の通信機能が停止する。したがって、携帯電話機の所有者が、その携帯電話機を紛失したり、盗難にあった場合でも、第３者が通信を行って過大な請求が携帯電話機の所有者に課せられる等の不具合を防止することができる。ステップＳ３１０を経ると、通常モードへ戻る。なお、他の処理についても、同様にサブルーチンで実行され、その基本的な内容は前記実施例と同様であり、サブルーチンの図示は省略する。ステップＳ３０８でＮＯのときはステップＳ３１２に進む。

【００５６】ステップＳ３１２では、設定済み誤入力に対する処理の解析結果が「記憶内容表示プロテクト」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３１４に分岐して「記憶内容表示プロテクト」の処理を実行する。ステップＳ３１２でＮＯのときはステップＳ１６に進む。「記憶内容表示プロテクト」の処理を実行することにより、ユーザー記憶エリア（所有者のプライベートデータや業務上の機密データを記憶）に対するアクセスが禁止される。また、記憶内容をクリアするようにしてもよい。したがって、パスワードの誤入力が３回以上あった場合、該当するユーザー記憶エリアを選択する制御信号が常にディスエーブルとなり、仮に第３者がアクセスしても、意味のないデータしか得ることができず、所有者のプライベートデータや業務上の機密データが記憶されていても、第３者によって公にされたり、悪用されたりするのを防止することができる。ステップＳ３１４を経ると、通常モードへ戻る。

【００５７】ステップＳ３１６では、設定済み誤入力に対する処理の解析結果が「所有者連絡先表示」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３１８に分岐して「所有者連絡先表示」の処理を実行する。ステップＳ３１６でＮＯのときはステップＳ３２０に進む。「所有者連絡先表示」の処理を実行することにより、表示部の表示がオンし、図９に示すような所有者連絡先が表示される。したがって、携帯電話機の置き忘れ等により紛失した場合には、この表示を出すことにより、所有者に対して携帯電話機６２を取得した人が連絡することが可能になる。ステップＳ３１８を経ると、通常モードへ戻る。

【００５８】ステップＳ３２０では、設定済み誤入力に対する処理の解析結果が「アラーム音発生」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３２２に分岐して「アラーム音発生」の処理を実行する。ステップＳ３２０でＮＯのときはステップＳ３２３に進む。「アラーム音発生」の処理を実行することにより、アラーム音発生のフラグがオンし、携帯電話機からアラーム音が発生し、周囲に知らせる。その結果、例えばアラーム音を聞いて第３者が紛失場所（例えば、路上）にある携帯電話機に気付くことも可能なる。ステップＳ３２２を経ると、通常モードへ戻る。

【００５９】ステップＳ３２４では、設定済み誤入力に対する処理の解析結果が「パワーオン禁止」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３２６に分岐して「パワーオン禁止」の処理を実行する。ステップＳ３２４でＮＯのときはステップＳ３２８に進む。「パワーオン禁止」の処理を実行することにより、マニュアルにして携帯電話機のスイッチをオンにしても、制御部のマイクロコンピュータはパワーオンシーケンスにてパワーオン禁止フラグをチェックし、即座にオフへと遷移する。したがって、携帯電話機が盗難にあってもすぐに使用できない状態にすることができ、第３者が通信を行って過大な請求が携帯電話機の所有者に課せられる等の不具合を防止することができる。ステップＳ３２６を経ると、通常モードへ戻る。

【００６０】ステップＳ３２８では、設定済み誤入力に対する処理の解析結果が「記憶内容送信」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３３０に分岐して「記憶内容送信」の処理を実行する。ステップＳ３２８でＮＯのときはステップＳ３３２に進む。「記憶内容送信」の処理を実行することにより、携帯電話機からパーソナルコンピュータの記憶媒体（例えば、フロッピィディスク、あるいはハードディスク）に携帯電話機の記憶内容が複写あるいは転送され、個人のスケジューラーや住所録等バックアップファイルを持っていないデータ等を携帯電話機から簡単に自分のパーソナルコンピュータの記憶媒体に複写あるいは転送することができ、貴重なデータの紛失を防ぐことができる。ステップＳ３３０を経ると、通常モードへ戻る。

【００６１】ステップＳ３３２では、設定済み誤入力に対する処理の解析結果が「端末の所在エリア送信」のコードであるか否かを判別し、ＹＥＳのときはステップＳ３３４に分岐して「端末の所在エリア送信」の処理を実行する。ステップＳ３３２でＮＯのときはシステムをオフし、通常モードへ戻る（リターン）。「端末の所在エリア送信」の処理を実行することにより、携帯電話機では公衆／専用回線網に接続された基地局の所在エリアを公衆／専用回線網を介して自分のパーソナルコンピュータに送信する。これにより、携帯電話機を管轄する基地局の位置が判明する。ステップＳ３３４を経ると、通常モードへ戻る。以上のように第３実施例では、所有者以外のものが携帯電話機を拾ったり、盗すんだりした場合に、その携帯電話機を使用しようとして誤ったパスワードの入力を３回以上繰り返すと、所有者によって予め設定された値に従い、あたかもリモート操作データを受信した場合と同様に、上述した各種のセキュリティ処理が実行される。したがって、前記第２実施例と同様の効果を得ることができる。

【００６２】なお、「通信機能プロテクト」、「記憶内容表示プロテクト」、「所有者連絡先表示」、「アラーム音発生」、「パワーオン禁止」、「記憶内容送信」、「端末の所在エリア送信」という各モードリティ処理は

全てを自動的に行ってもよいし、あるいはこれらのセキュリティ処理のうち、何れか1つ（又は1つ以上）を自動的に行うようにしてもよい。また、同時に送信回路を用いて、所有者に対して他の者によって誤入力がなされたことを知らせることようにしてもよい。そのようにすると、より一層、携帯電話機に対するセキュリティの実効を高めることができる。上記第2、第3実施例は携帯端末装置に対するセキュリティとして、携帯電話機を例にしているが、携帯電話機に限るものではなく、例えば携帯型コンピュータ（テレターミナル型やパームトトップ型の小型コンピュータ）あるいはページャに対しても適用することができ、同様の効果を得ることが可能である。

【００６３】本発明の第４実施例

次に、本発明の第４実施例について説明する。本実施例は、携帯端末装置を悪用防止機能を備えたページャーに適用した例である。

Ａ．本実施例の背景

一般に、ページャーは個人単位での使用に対するサービスの一般化と、技術革新による小型化、軽量化、多機能化により、汎用性、携帯性優れ、簡易で経済的な移動体通信手段として広く普及しつつある。ところで、簡易かつ便利な移動体通信手段としてページャーが普及するにつれ、紛失あるいは盗難等の予期せゆ事態に所有者が遭遇するケースが増えたにもかかわらず、実際には利用しているサービス会社への届け出以外、即座に対応できる対応手段に乏しいものであった。また、万一、第３者が紛失等したページャーを発見し、取得した場合でも、所有者の氏名や連絡先等、取得者に伝えられべき情報が表示されず、最悪の場合にはページャー内部に記憶されている所有者個人宛てのメッセージを見られたり、受信されたり、電話番号の悪用等、所有者のプライバシーや、機密の漏洩等、個人の信用に関わる問題が発生する危険性があった。

【００６４】Ｂ．ページャーの構成

図１６はページャー１００の本体内部の電子回路を構成するブロック図である。図１６において、ページャー１００は大きく分けてＣＰＵ１０１、アンテナ１０２、ＲＦ受信部１０３、デコーダ部１０４、ＩＤ－ＲＯＭ１０５、ＲＯＭ１０６、キー入力部１０７、表示バッファ１０８、表示部１０９、ＲＡＭ１１０、スピーカードライバ１１１、スピーカー１１２、バイブレータドライバ１１３、バイブレータ１１４、ＬＥＤドライバ１１５およびＬＥＤ１１６により構成される。ＣＰＵ（機能制限手段）１０１は各回路を制御し、セキュリティ処理に必要な機能を実現する。ＲＦ受信部１０３はアンテナ１０２で受信された電波を復調してデコーダ部１０４に出力する。ＩＤ－ＲＯＭ１０５は当該ページャー１００に個別に割り当てられているフレームやアドレス等を記憶し、デコーダ部１０４の制御の下に記憶しているフレームやアドレス等をデコーダ部１０４に送出する。デコーダ部１０４はＲＦ受信部１０３で受信された復調された受信信号をＩＤ－ＲＯＭ１０５からのデータと照合し、その受信信号が自己に対して送られてきたものであるときには、一致信号をＣＰＵ１０１に出力する。アンテナ１０２、ＲＦ受信部１０３およびデコーダ部１０４は特定信号検出手段を構成する。

【００６５】キー入力部１０７は文字数字キー、ファンクションキー等からなるキーボード部分と、各種スイッチ部分で構成されており、キーボード部分については、ある入力がなされると、ＣＰＵ１０１で処理され、液晶パネルを駆動させる回路を含む表示バッファ１０８を通して液晶表示パネルを備えた表示部（特定情報表示手段）１０９に、特定メッセージとして表示されるだけでなく、ＲＡＭ１１０に記憶させることができる。なお、表示部１０９はドット表示であれば、漢字による表示も可能である。また、各種スイッチ部分は呼出しを受信したときに呼出音を発生する鳴音モードと、呼出音を発生しない無音モードとの間でモードの切替を行うモード切替スイッチ、呼出音の発生を停止させるときに操作するリセットスイッチ等で構成されている。

【００６６】ＬＥＤドライバ１１５はＣＰＵ１０１からの制御信号を受けてＬＥＤ１１６を駆動するものである。ＬＥＤ１１６はＬＥＤドライバ１１５に駆動されて点滅あるいは点灯して受信報知を行う。スピーカードライバ１１１はＣＰＵ１０１からの制御信号を受けてスピーカー１１２を駆動するものである。スピーカー１１２はスピーカードライバ１１１により駆動されて呼出音を発生させる。バイブレータドライバ１１３はＣＰＵ１０１からの制御信号を受けてバイブレータ１１４を駆動するものである。バイブレータ１１４はバイブレータドライバ１１３により駆動されて振動する振動装置で、振動によって受信を知らせる。ＲＯＭ（特定情報記憶手段）１０６には予めサービス会社の社名、住所、電話番号等の特定メッセージが記憶されるとともに、ＣＰＵによって実行されるメッセージ受信処理の他にセキュリティ処理のプログラムが記憶されている。なお、特定信号受信時はＲＡＭ１１０に特定メッセージデータが記憶されていない場合に限り、表示部１０９に表示される。

【００６７】ＲＡＭ１１０は主に過去の受信データ等を記憶する受信情報エリアＣＭと、作成した特定メッセージを記憶する特定受信エリアＳＭとで構成されている。図１７はＲＡＭ１１０のレジスタ構成を示す図である。図１７において、バッファレジスタＢＲはデコーダ部１０４からＣＰＵ１０１に送られてきた受信データが一旦セットされるレジスタである。その下のエリアには、呼出音の発生等のときに立てられ、リセットボタンを押すことで下ろされるリセットフラグＲＳ１、特定信号での呼出音の発生のときに立てられ、リセットボタンを押すことで下ろされるリセットフラグＲＳ２、表示部１０９

に受信メッセージ等が表示されているときに立てられる表示フラグD、ＬＥＤ１１６等による受信報知を行っているときに立てられる報知フラグA、鳴音モードのときに立てられ、無音モードのときに下ろされるモードフラグＭＦ、受信情報ＣＭの各行を指定するポインタＰ等を配している。ワークエリアWは大きく２つのエリア、すなわち受信情報エリアＣＭと、特定受信エリアＳＭとに分れている。受信情報エリアＣＭは通常の信号を受信したときに動作する電話番号エリアＴＮ、メッセージエリアＭＡ、ＣＰＵ１０１により計時される受信時刻エリアＲＴ等を備えている。一方、特定受信エリアＳＭは特定信号を受信したときのみ呼び出される特定メッセージエリアＴＡ、特定信号受信時刻エリアＲＴＳ等を備えている。

【００６８】Ｃ．ページャーのセキュリティ動作

当該ページャー１００についての通常の動作は、一般に普及しているページャーと同様である。図１８はページャー１００のセキュリティ処理を示すフローチャートであり、所有者が当該ページャー１００を紛失若しくは盗難等の予期せぬ事態に遭遇したケースについてのものである。所有者がページャー１００を紛失若しくは盗難等の予期せぬ事態に遭遇した場合、ページャー１００はステップＳ４００で既に電源がオンし、着信待ちの状態になっているものとする。次いで、ステップＳ４０２に進み、所有者が外部より公衆電話回線を使用して特定信号（例えば、セキュリティ処理の実行を命令する信号）をページャー１００へ送信すると、当該ページャー１００では、この特定信号をアンテナ１０２で受けて、特定信号の着信を行い、ＲＦ受信部１０３で復調する。次いで、ステップＳ４０４でデコーダ部１０４において復調された信号をＩＤ－ＲＯＭ１０５によって照合し、ＩＤ－ＲＯＭ１０５に予め記憶されているＩＤ特定コードと一致するか否かを判別する。一致しなければ、ステップＳ４００に戻ってループを繰り返し、一致すると、ステップＳ４０６に抜ける。このとき、デコーダ部１０４からＣＰＵ１０１へ一致したことを示す信号が出力される。

【００６９】ステップＳ４０６ではセキュリティ処理として、以下の処理命令を出力する。

①キー入力部１０７による入力機能の停止

これにより、第３者がキー入力部１０７を操作して表示部１０９にデータを表示させる等の命令を入力しようとしても、全くキー入力ができず、悪用が防止される。

②デコーダ部１０４からの通常信号の受信機能の停止

これにより、受信メッセージ等を受信することができなくなり、悪用が防止される。

③報知機能の始動

これにより、ＬＥＤドライバ１１５が駆動され、ＬＥＤ１１６により特定信号の受信が報知される。また、スピーカドライバ１１１によりスピーカ１１２が駆動されて特定信号の受信が報知される。さらに、バイブレータドライバ１１３によりバイブレータ１１４が駆動され、特定信号の受信が振動によって伝達される。

【００７０】④ＲＡＭ１１０への受信コード出力機能の停止

これにより、ＲＡＭ１１０による受信コードの記憶ができず、例えば他人から所有者に向けて発信されたメッセージ等がページャー１００を取得した第３者に明らかになることがなくなる。

⑤特定メッセージの表示

これにより、ＲＡＭ１１０に予め記憶されている特定メッセージを表示部１０９に表示する命令が出力される。なお、ＲＡＭ１１０に特定メッセージが記憶されていない場合には、ＲＯＭ１０６に予め記憶されているサービス会社の社名、住所、電話番号等の特定メッセージを表示する命令が出力される。次いで、ステップＳ４０８に進み、特定メッセージを表示部１０９に表示する。ステップＳ４０８を経ると、ルーチンを終了する。最終的に特定信号を受信したページャー１００はステップＳ４０８の状態で、例えば図１９に示すような特定メッセージ等を表示部１０９に表示する。図１９の例では、拾い主に対して終所有者の氏名、住所、連絡先等を知らせるメッセージ内容になっている。

【００７１】以上の操作により、ページャー１００が紛失若しくは盗難等、予期せゆ事態に所有者が遭遇しても、第３者が紛失したページャーを発見し、取得した場合には、所有者の氏名や連絡先等、取得者に伝えられべき情報が表示されるから、第３者への早期発見、所有者への返却を促すことができる。また、ページャー１００の内部に記憶されている所有者個人宛てのメッセージの表示を禁止したり、キー入力の禁止したりするから、所有者への個人宛てのメッセージを見られたり、受信されたり、電話番号の悪用等、所有者のプライバシーや、機密の漏洩等、個人の信用に関わる問題の発生を未然に防止して、第３者によるページャー１００の悪用を防止することができる。なお、本実施例におけるセキュリティ処理対象の携帯端末装置はページャーになっているが、本実施例のようなセキュリティ処理は、例えば携帯端末用通信機器、あるいは移動体通信機器の端末等でも、本発明の目的の範囲内で適用できる。

【００７２】本実施例は携帯端末装置をＰＨＰに適用した例であるが、本発明はＰＨＰに限らず、他の携帯端末装置（例えば、家庭用のコードレス電話機）にも幅広く適用できるのは勿論である。また、電話機１とＰＨＰ２との間の同一所有性を確認する方法は、上記実施例の例に限らず、他の方法を用いてもよい。例えば、各保護処理に対応した保護用の暗証番号を設けて、同一所有者と保護処理内容を同時に転送して確認してもよいし、保護処理をするための特別のＩＤコードに暗証番号と制御内容を付加してもよい。さらに、装置を構成する各部材の

種類・個数、制御方法等は、どのようなものでもよいことは言うまでもない。本発明を発展的形態として、例えば電話機1からでなく、緊急の場合には通常どこにでもある公衆電話からでも所定の暗証番号等を入力することにより、リモート操作により、本発明と同様の保護処理を行うことがてきるようにしてもよい。

【0073】

【発明の効果】本発明によれば、以下の効果を得ることができる。

(1)携帯端末装置を紛失した場合、その所有者が外部からリモート指令を入力して携帯端末装置をリモート操作することにより、携帯端末装置側の保護処理手段により携帯端末装置の所有者が不利になることを排除する保護処理を実行しているので、携帯端末装置を紛失しても外部からの指令で、携帯端末装置を紛失した場合に生じる諸問題を適切にクリアすることができる。

(2)すなわち、簡単に携帯端末装置内部のデータを保護することができるとともに、他人に使用されて課金されるという不具合を防止することができる。

(3)具体的には、取得者が勝手に電話をかけまくるというような事態を防ぐことができ、通話料金の請求について携帯端末装置の契約者に回されることを最小限に抑えることができる。

(4)その結果、使用していないにもかかわらず料金を支払らわなければないないという事態を避けて、他人に使用されて課金されるという不具合を防止することができる。

(5)所有者が携帯端末装置の紛失あるいは盗難に気付いた場合、所有者による積極的なセキュリティ活動（例えば、リモート操作データの送信）を行うことによって、携帯端末装置の所有者に不利益となる要因を防止することができる。すなわち、携帯端末装置の記憶内容および使用に関してプロテクトをかけて保護することができる。

(6)所有者が携帯端末装置の紛失又は盗難に気が付いた場合、公衆（あるいは専用）通信ネットワークを形成している事業者を通して携帯端末装置に記憶された所有者のデータを回収することができる。

(7)受信した信号に特定の信号がある否かを判別し、特定信号が検出されると、その携帯端末装置の機能を制限するようなセキュリティ処理を実行しているので、所有者と携帯端末装置との間に予期せぬ事態が発生（例えば、紛失、盗難）した場合、外部より公衆電話回線を用いて特定信号を送信することにより、通信機能を制限でき、第3者に悪用される危険性を無くすことができる。

【図面の簡単な説明】

【図1】本発明に係る携帯端末装置の第1実施例のネットワーク構成図である。

【図2】同実施例のＰＨＰの詳細な構成を示すブロック図である。

【図3】本発明に係る携帯端末装置の第2実施例のネットワーク構成図である。

【図4】同実施例のセキュリティ処理の制御ルーチンを示すフローチャートである。

【図5】同実施例の携帯端末におけるリモート操作データの処理ルーチンを示すフローチャートである。

【図6】同実施例の通信機能プロテクトのサブルーチンを示すフローチャートである。

【図7】同実施例の記憶内容表示プロテクトのサブルーチンを示すフローチャートである。

【図8】同実施例の所有者連絡先表示のサブルーチンを示すフローチャートである。

【図9】同実施例の所有者連絡先表示の一例を示す図である。

【図10】同実施例のアラーム音発生のサブルーチンを示すフローチャートである。

【図11】同実施例のパワーオン禁止のサブルーチンを示すフローチャートである。

【図12】同実施例の記憶内容送信のサブルーチンを示すフローチャートである。

【図13】同実施例の端末の所在エリア送信のサブルーチンを示すフローチャートである。

【図14】本発明に係る携帯端末装置の第3実施例のパスワード設定ルーチンを示すフローチャートである。

【図15】同実施例のパスワード入力に対する機器の処理ルーチンを示すフローチャートである。

【図16】本発明に係る携帯端末装置の第4実施例のページャーの本体内部の電子回路を示すブロック図である。

【図17】同実施例のＲＡＭのレジスタ構成を示す図である。

【図18】同実施例のページャーのセキュリティ処理を示すフローチャートである。

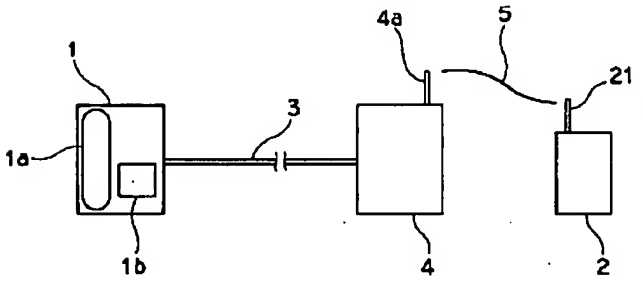
【図19】同実施例の特定メッセージの表示例を示す図である。

【符号の説明】

1　電話機
1b　キー操作部
2　ＰＨＰ（携帯用の子機電話）
3　有線の通信回線
4　中継局
5　無線通信回線
11　制御部（保護処理手段、一致指令手段）
14　キー入力部（特定データ指定手段）
15　表示部
17　メモリ
22　高周波部
23　モデム
24　ＴＤＭＡ信号処理部
25　スピーチコーデック

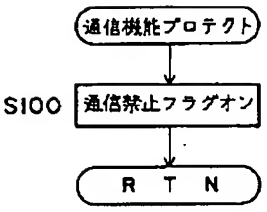
２６　ＰＣＭコーディック
３１　受信部（受信手段）
３２　送信部
５３　パーソナルコンピュータ
５７　網管理局
６２　携帯電話機（通信手段、操作データ認識手段、セキュリティ手段、パスワード解析手段、誤入力報知手段）
１００　ページャー（携帯端末装置）
１０１　ＣＰＵ（機能制限手段）
１０３　ＲＦ受信部
１０４　デコーダ部
１０５　ＩＤ－ＲＯＭ
１０６　ＲＯＭ（特定情報記憶手段）
１０７　キー入力部
１０９　表示部
１１０　ＲＡＭ
１１４　表示部（特定情報表示手段）

【図１】

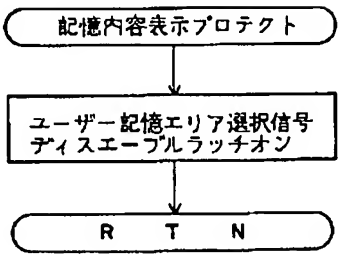



【図２】

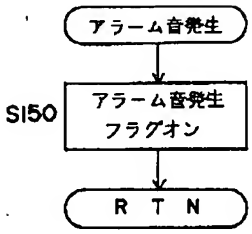
【図６】



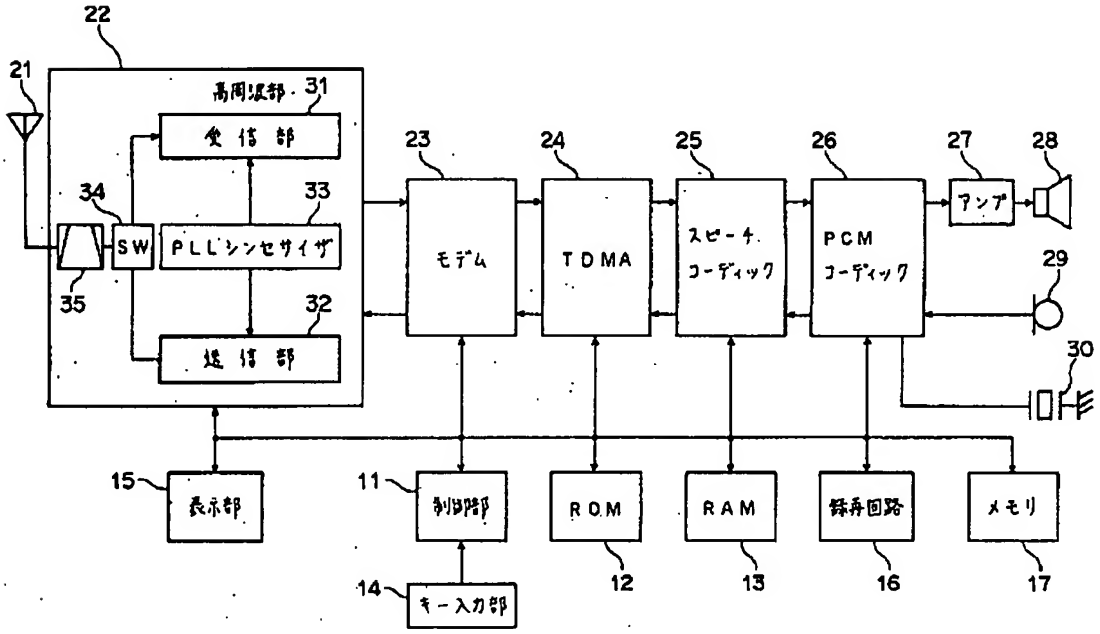

【図７】




【図１０】

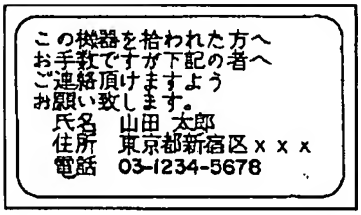


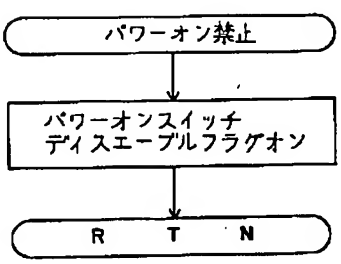

【図９】

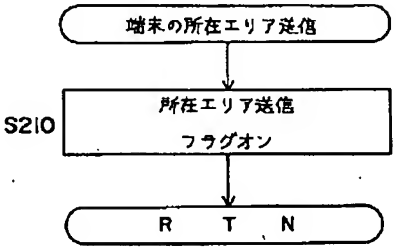



【図１１】

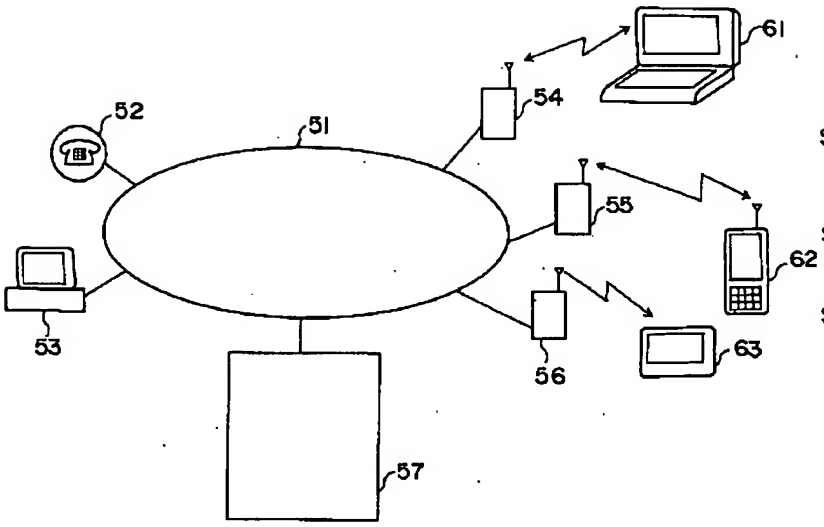
【図１３】



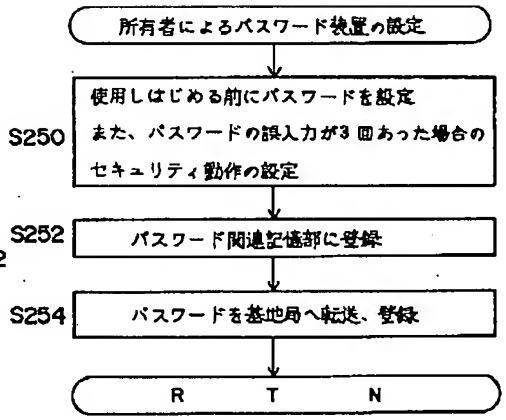



【図３】

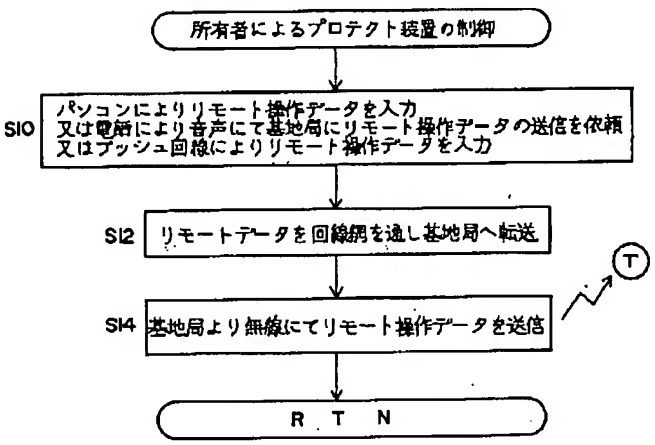



【図１４】

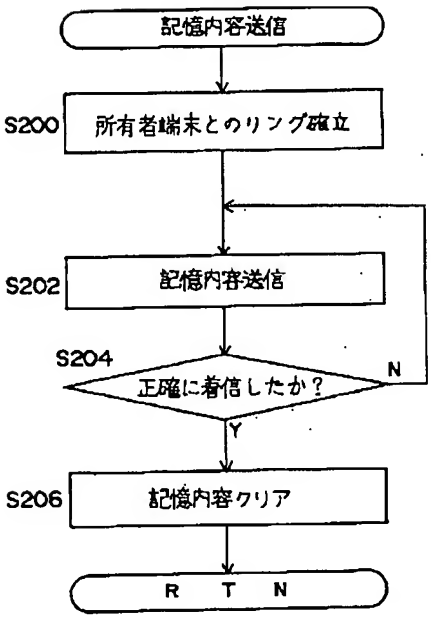


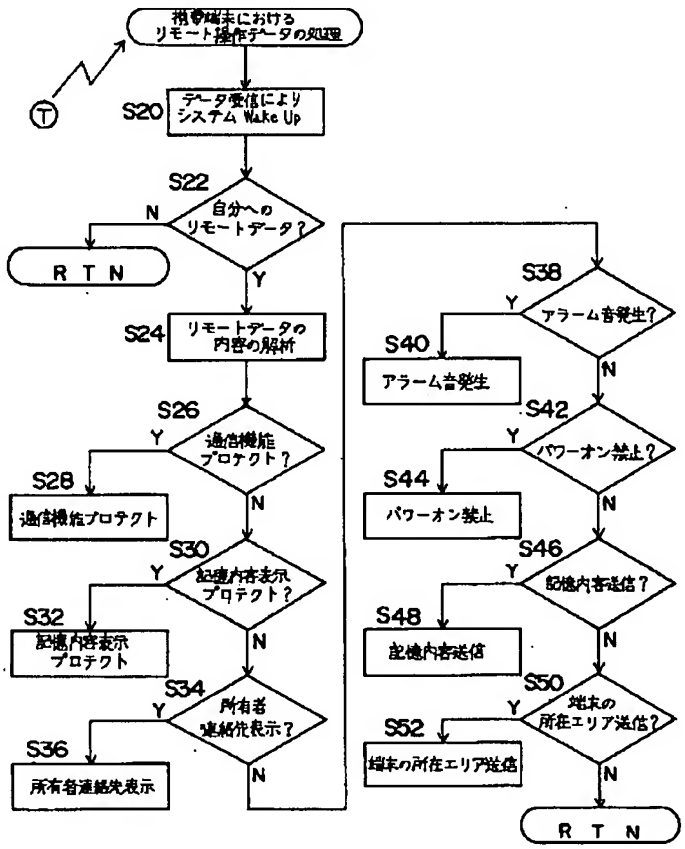

【図４】

【図５】

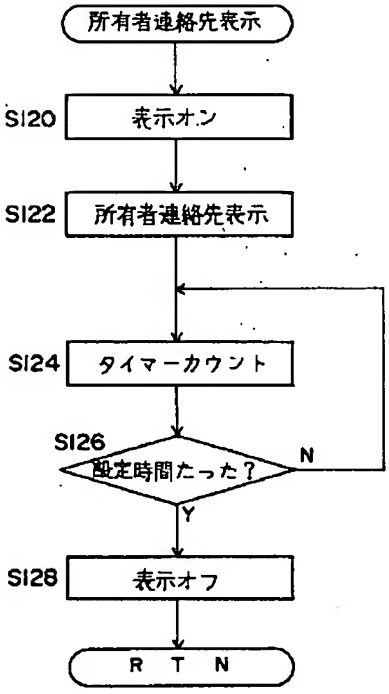



【図１２】

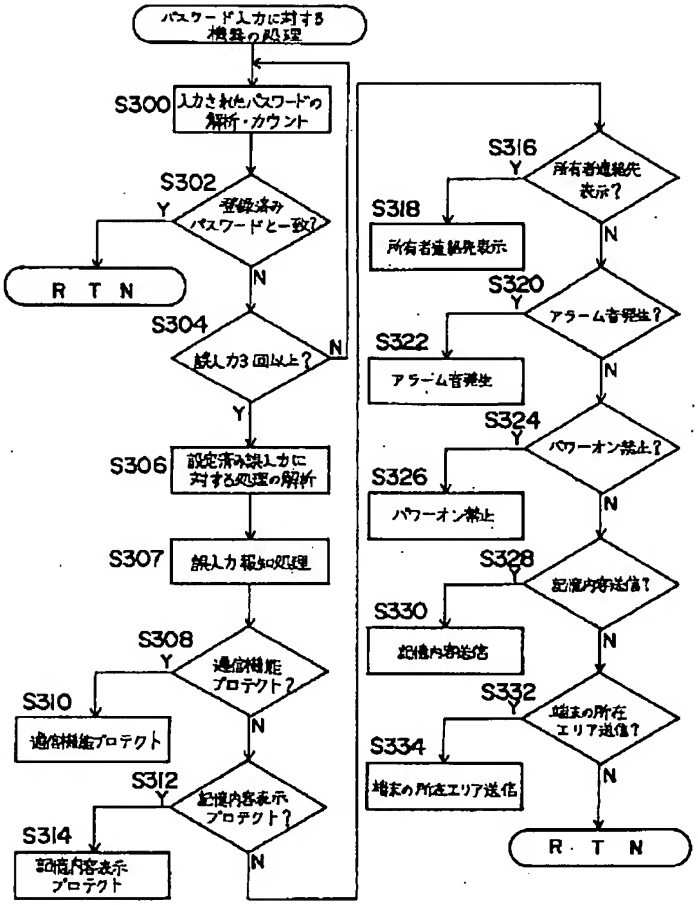


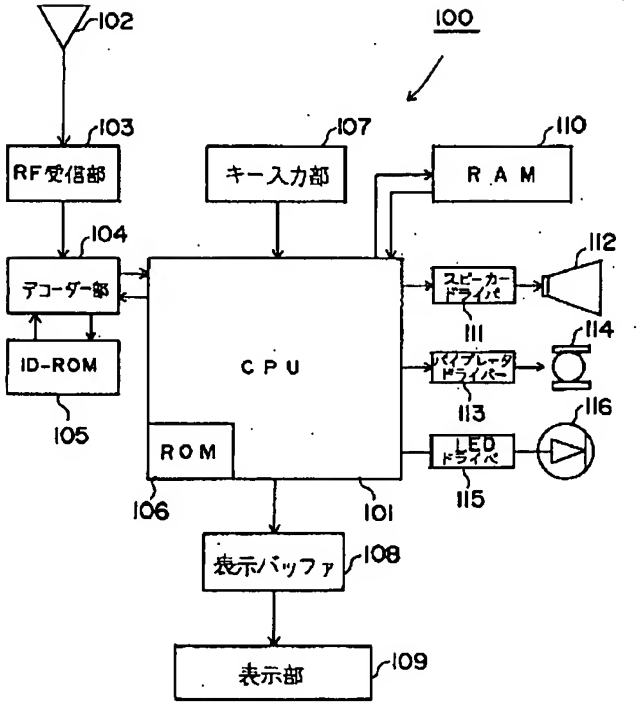
【図８】



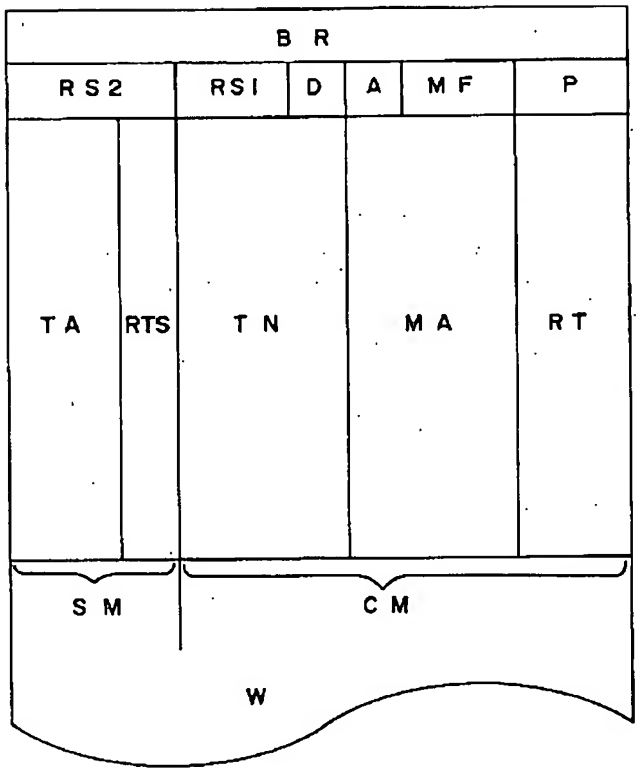

【図１５】



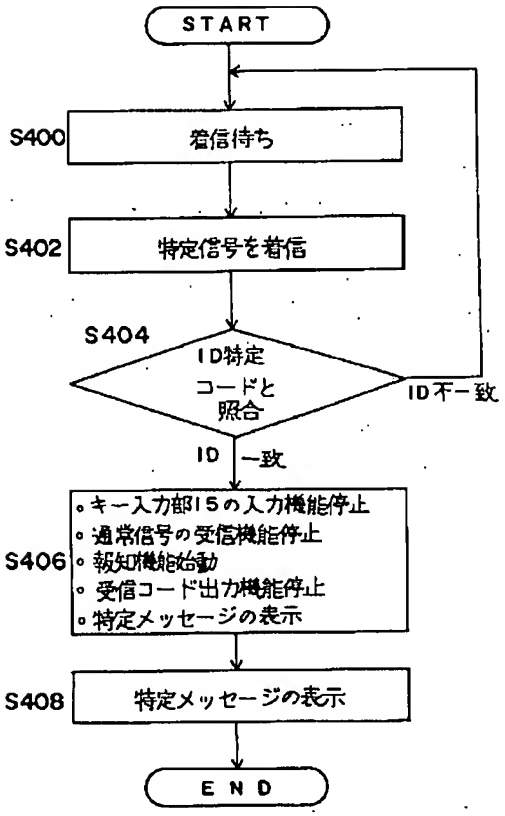

【図１６】



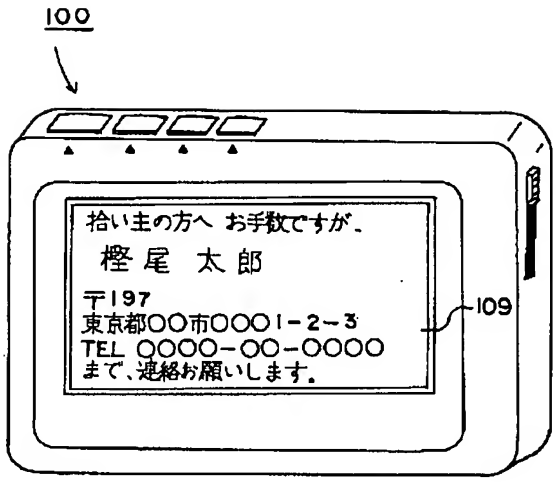

【図１７】



【図１８】




【図１９】




---

フロントページの続き

(72)発明者　折本　孝
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(72)発明者　金子　克義
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(72)発明者　渡辺　一嘉
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(72)発明者　廣谷　孝幸
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１４年１月１１日（２００２．１．１１）

【公開番号】特開平７－１９３８６５
【公開日】平成７年７月２８日（１９９５．７．２８）
【年通号数】公開特許公報７－１９３９
【出願番号】特願平６－１７００９５
【国際特許分類第７版】
　C08L　83/06　　LRP
　B29D　31/00
　C08K　 3/20
　　　　 5/05
　　　　 5/54
　C08L　83/05　　LRQ
　　　　83/07
　F16C　13/00
// B29K　83:00
　H04Q　 7/38
　H04M　 1/00
【ＦＩ】
　C08L　83/06　　LRP
　B29D　31/00
　C08K　 3/20
　　　　 5/05
　　　　 5/54
　C08L　83/05　　LRQ
　　　　83/07
　H04B　 7/26　　109 R
　H04M　 1/00　　　N

【手続補正書】
【提出日】平成１３年６月２６日（２００１．６．２６）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　外部より通信回線を介してリモート操作データを受信し、
受信したリモート操作データの内容に基づいて、
所定の連絡先に連絡するための処理を行い、
この処理に基づき、前記所定の連絡先に連絡を行うことを特徴とする携帯端末装置のセキュリティ方法。
【請求項２】　外部より通信回線を介して入力されたリモート操作データに基づいて、所定の連絡先に連絡するための処理を行う処理手段と、
この処理に基づき、前記所定の連絡先に連絡する連絡手段を設けたことを特徴とする携帯端末装置。
【請求項３】　前記処理手段は、外部より通信回線を介して入力された暗証番号の一致が確認された後に、前記処理を行うことを特徴とする請求項２記載の携帯端末装置。
【請求項４】　前記連絡手段は、当該携帯端末装置の使用に応じて、前記所定の連絡先に連絡を行うことを特徴とする請求項２又は３記載の携帯端末装置。
【請求項５】　データ通信可能な通信手段と、
この通信手段を介して送信されてきたデータのうちリモート操作データを判別する判別手段と、
この判別手段により判別されたリモート操作データにより所定の送信処理行うためのセキュリティ処理を実行するセキュリティ手段と、
を備えたことを特徴とする携帯端末装置。
【請求項６】　前記セキュリティ手段は、
ａ．当携帯端末装置の概略の所在地を所有者に知らせるデータ送信処理

b．当該携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理
のうちのいずれかあるいは全ての送信処理を行うためのセキュリティ処理を実行することを特徴とする請求項5記載の携帯端末装置。
【請求項7】　パスワードを入力するパスワード入力手段と、
このパスワード入力手段により入力されたパスワードの正誤を判別するパスワード解析手段と、を備え、
前記セキュリティ手段は、前記パスワード判別手段によりパスワードが誤りと判別された場合に、前記a～bの全てあるいは1つ以上の送信処理を行うことを特徴とする請求項6記載の携帯端末装置。
【請求項8】　データ通信可能な通信手段と、
パスワードを入力するパスワード入力手段と、
入力されたパスワードの正誤を判別するパスワード判別手段と、
このパスワード判別手段によりパスワードの誤入力が判別された場合、
a．携帯端末装置の所在地を所有者に知らせるデータ送信処理
b．携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理
のうちの全てあるいは1つ以上の所定の少なくとも何れかを実行することを特徴とする携帯端末装置。
【請求項9】　所有者にパスワードの誤入力があったことを知らせる誤入力報知手段を備えていることを特徴とする請求項8記載の携帯端末装置。
【手続補正2】
【補正対象書類名】明細書
【補正対象項目名】0005
【補正方法】変更
【補正内容】
【0005】
【課題を解決するための手段】上記目的達成のため、請求項1記載の発明による携帯端末装置のセキュリティ方法は、外部より通信回線を介して入力されたリモート操作データを受信し、受信したリモート操作データの内容に基づいて、所定の連絡先に連絡するための処理を行い、この処理に基づき、前記所定の連絡先に連絡を行うことを特徴とする。請求項2記載の携帯端末装置は、外部より通信回線を介して入力されたリモート操作データに基づいて、所定の連絡先に連絡するための処理を行う処理手段と、この処理に基づき、前記所定の連絡先に連絡する連絡手段を設けたことを特徴とする。
【手続補正3】
【補正対象書類名】明細書
【補正対象項目名】0006
【補正方法】変更
【補正内容】
【0006】好ましい態様として、例えば請求項3記載のように、前記処理手段は、外部より通信回線を介して入力された暗証番号の一致が確認された後に、前記処理を行うようにしてもよい。また、例えば請求項4記載のように、前該携帯端末装置の使用に応じて、前記所定の連絡先に連絡を行うこととしてもよい。
【手続補正4】
【補正対象書類名】明細書
【補正対象項目名】0007
【補正方法】変更
【補正内容】
【0007】請求項5記載の携帯端末装置は、データ通信可能な通信手段と、ためこの通信手段を介して送信されてきたデータのうちリモート操作データを判別する判別手段と、この判別手段により判別されたリモート操作データにより所定の送信処理を行うためのセキュリティ処理を実行するセキュリティ手段と、を備えたことを特徴とする。また、例えば請求項6記載のように、前記セキュリティ手段は、a．当該携帯端末装置の所在地を所有者に知らせるデータ送信処理b．当該携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理のうちの全てあるいは1つ以上の送信処理を行うのセキュリティ処理を実行するようにしてもよい。
【手続補正5】
【補正対象書類名】明細書
【補正対象項目名】0008
【補正方法】変更
【補正内容】
【0008】例えば請求項7記載のように、パスワードを入力するパスワード入力手段と、このパスワード入力手段により入力されたパスワードの正誤を判別するパスワード判別手段と、を備え、前記セキュリティ手段は、前記パスワード判別手段によりパスワードが誤りと判別された場合に、前記a～bの全てあるいは1つ以上の送信処理を行うためのセキュリティ処理を実行するようにしてもよい。請求項8記載の携帯端末装置は、データ通信可能な通信手段と、パスワードを入力するパスワード入力手段と、入力されたパスワードの正誤を判別するパスワード判別手段と、このパスワード判別手段によりパスワードの誤入力が判別された場合、
a．携帯端末装置の所在地を所有者に知らせるデータ送信処理
b．携帯端末装置に内蔵されている記憶手段の内容を、他の通信機能を有する端末に送信する送信処理
のうちの全てあるいは1つ以上の所定の少なくとも何れかを実行することを特徴とする。例えば請求項9記載のように、所有者にパスワードの誤入力があったことを知らせる誤入力報知手段を備えるようにしてもよい。
【手続補正6】

【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】削除
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】削除
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正内容】
【００１１】
【作用】本発明では、携帯端末装置を紛失した場合等、その所有者あるいは通信事業者等によって通信回線を介してリモート操作データが入力され、受信したリモート操作データの内容に基づいて、所定の連絡先に連絡するための処理を行い、この処理に基づき、前記所定の連絡先に連絡を行う。この処理は、例えば、外部より通信回線を介して入力された暗証番号の一致が確認された後に行われる。連絡するための処理としては、例えば携帯端末装置を使用すると、予め記憶された連絡先につながるようにする処理が行われる。したがって、携帯端末装置を紛失しても所有者あるいは通信事業者からの指令で、予め記憶された連絡先につながるようになり、かつ他人に使用されて不必要に課金される等という不具合を防止できる。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正内容】
【００１２】また、請求項５記載の発明では、送信されたデータのうちのリモート操作データにより、所定の送信処理を行うためのセキュリティ処理を実行するセキュリティ手段を有する。例えば請求項６記載の発明では、携帯端末装置の所在を所有者に連絡したり、当該携帯端末装置に内蔵されている記憶手段の内容を他の通信機能を有する端末に送信する処理が実行される。したがって、携帯端末装置を紛失・盗難等の場合でも、有用なデータを回収することができる。また、請求項７記載の発明では、入力されたパスワードが誤りと判別された場合に送信処理がおこなわれる。また、請求項８記載の携帯端末装置は、パスワードの誤入力が判別された場合に、
ａ．携帯端末装置の所在地を所有者に知らせるデータ送信処理
ｂ．携帯端末装置に内蔵されている記憶手段の内容を他の通信機能を有する端末に送信する送信処理のうちの何れかが実行される。したがって、携帯端末装置を紛失・盗難等の場合でも、携帯端末装置の所在地を知ることができる、又は有用なデータを回収することができる。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００７３
【補正方法】変更
【補正内容】
【００７３】
【発明の効果】本発明によれば、以下の効果を得ることができる。
１．携帯端末装置を紛失した場合、その所有者等が外部からリモート指令を入力して携帯端末装置をリモート操作することにより、携帯端末装置に所定の連絡先に連絡するための処理を行うことができる。したがって、携帯端末装置を紛失しても外部からの指令で、携帯端末装置に所定の連絡先に連絡させることにより、携帯端末装置を紛失した場合に生じる諸問題を適切にクリアすることができる。
２．例えば、当該携帯端末装置が他人等に使用されたことに応じて、所有者等の連絡先に連絡を行うことができ、取得者が勝手に電話をかけまくるというような事態を防ぐことができ、通話料金の請求について携帯端末装置の契約者に回されることを最小限に抑えることができる。
３．例えば、所有者が携帯端末装置の紛失あるいは盗難に気付いた場合等例えば、リモート操作データの送信を行うことによって、携帯端末装置の所有者に不利益となる要因を防止することができる。
４．例えば、当該携帯端末装置の所在地を所有者に知らせることができる。
５．また例えば、携帯端末装置に記憶されたデータを回収することができる。したがって、携帯端末装置を紛失しても外部からの指令で、携帯端末装置を紛失した場合に生じる諸問題を適切にクリアすることができる。